VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Emulační model IP telefonní infrastruktury pro výuku

The Simulation Model of IP Telephony Infrastrukture for Education

2017 **Bc. Richard Mlčoch**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Richard Mlčoch**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Emulační model IP telefonní infrastruktury pro výuku
The Simulation Model of IP Telephony Infrastructure for Education

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je navrhnout a vytvořit modulární model emulovaný v prostředí GNS3 za účelem vytváření IP telefonní infrastruktury pro výuku a předkonfigurovaných šablon pro praktická cvičení.

Zadání:

1. Detailně nastudujte možnosti tvorby emulačního modelu pro IP telefonii, GNS3, SIP protokol.
2. Navrhněte topologie IP telefonní infrastruktury s ohledem na modularitu a škálovatelnost.
3. Realizujte a nakonfigurujte návrh v podobě emulačních modelů v prostředí GNS3.
4. Proveďte testování funkčnosti a měření dílčích IP telefonních parametrů na modelu.
5. Vytvořte uživatelskou dokumentaci pro možnosti využití modelu ve výuce.

Seznam doporučené odborné literatury:

[1] The Practical OPNET User Guide for Computer Network Simulation by Adarshpal S. Sethi and Vasil Y. Hnatyshin (August 24, 2012)
[2] Network Simulation Experiments Manual, 5th Edition by Emad Aboelela (March 17, 2011)

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Filip Řezáč, Ph.D.**

Datum zadání: 01.09.2016

Datum odevzdání: 28.04.2017

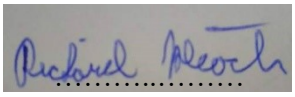
doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *23. dubna 2017*



……..……
podpis studenta

Poděkování

Rád bych poděkoval Ing. Filipu Řezáčovi, Ph.D. za odbornou pomoc a konzultace při tvorbě této diplomové práce.

Abstrakt

Tato diplomová práce se zabývá tvorbou IP telefonních emulačních modelů, které budou následně sloužit studentům ke snadnějšímu porozumění dané problematiky. Původní myšlenkou a podnětem ke vzniku práce byla skutečnost, že konfigurace telefonních modelů a samotná integrace jednotlivých software a hardware zařízení do jednoho celku neboli topologie, zabere na školních cvičeních až příliš prostoru, což zapříčiňuje vznik nedostatku času k potřebnému porozumění principu dané služby i funkčnosti jednotlivých technologií IP telefonie. Za tímto účelem byly navrhnuty, popsány a nakonfigurovány tři v praxi nejpoužívanější VoIP topologie s ohledem na modularitu a škálovatelnost. Cílem je úspora času, kdy si student otevře již předpřipravený emulovaný funkční telefonní model, kde si dle zadání provede potřebné operace a může se věnovat již samotnému testování a studiu dané problematiky namísto toho, aby začínal na každém cvičení úplně od začátku.

Klíčová slova

Emulace, GNS3, VirtualBox, Asterisk, Elastix, Kamailio, IP Telefonie, VoIP, Model, SIP

Abstract

This Master´s Thesis focuses on creation IP telephony emulation models which will be used by students for easier understanding of this problem. The original idea why I have decided to create this Thesis was the fact that configuration of telephony models and integration of SW and HW unit to the whole complex or topology take a lot of practise time so there is not enough time for understanding how the technology of IP telephony works. For this purpouse three most used VOIP topology were designed, described and configured due to modularity and scalability. The main aim is the time saving. Student can open pre-prepared functional emulated phone model and starts with testing and studing this problem immediately after a few needed activities instead of doing all his work completely from the beginning.

Key words

Emulation, GNS3, VirtualBox, Asterisk, Elastix, Kamailio, IP Telephony, VoIP, Model, SIP

Obsah

Seznam použitých zkratek

Zkratka	Význam
ASA	Adaptive Security Appliance. Cisco software pro firewall a síťovou ochranu.
ATM	Asynchronous Transfer Mode. Standart pro síťovou architekturu.
CRM	Customer Relationship Management. Zákaznicky orientovaný management.
CUCME	Cisco Unified Communications Manager Express.
DHCP	Dynamic Host Configuration Protocol. Automatické přiřazení IP adres.
DNS	Domain Name System. Převod domén na IP adresy.
DSL	Digital Subscriber Line. Přenos dat pomocí stávajícího telefonního vedení.
DTMF	Dual Tone Multi-Frequency. Způsob kódování a přenosu tel. čísla.
GNS3	Graphical Network Simulator 3. Emulační software.
GPL	General Public Licence. Všeobecná veřejná licence.
GUI	Graphical User Interface. Ovládání počítače pomocí grafických prvků.
HTML5	Programovací jazyk sloužící pro tvorbu webových stránek.
IAX	Inter-Asterisk eXchange. Komunikační protokol využívaný Asteriskem.
IBM	International Business Machines. Počítačová společnost.
ID	Identifikační číslo.
IOS	Operační systém používaný na směrovačích a přepínačích firmy Cisco.
IP	Internetový protokol. Základní komunikační protokol internetu.
IPS	Instruction Prevention System. Systém pro prevenci a detekci před útoky.
IVR	Interactive Voice Response. Funkce interaktivní hlasové odezvy.
JUNOS	Operační systém používaný ve směrovačích firmy Juniper.
MGCP	Media Gateway Control Procol. Komunikační protokol používaný ve VoIP.
MYSQL	Systém řízení báze dat uplatňující relační databázový model.
NAC	Network Access Control. Počítačová bezpečnost zahrnující antivirus atd.
OS	Operační systém.
PBX	Private Branch Exchange. Sjednocuje výstupní body telefonů do jedné sítě.
PIX	Private Internet eXchange. Populární firewall využívaný spol. Cisco.
PSTN	Public Switched Telephone Network. Veřejná telefonní síť.
QOS	Quality of Service. Řízení datových toků v telekomunikačních a dat. sítích.

RAM	Random-access memory. Slouží procesoru pro efektivní práci s daty.
RFC	Request For Comments. Pravidla neboli dokumenty pro fungování internetu.
RTP	Real-time Transport Protocol. Protokol přenášející hlasový tok.
SCCP	Skinny Client Control Protocol. Komunikační protokol firmy Cisco.
SEMS	Sip Express Media Server. Telefonní server podporující SIP technologii.
SIP	Session Initiation Protocol. Signalizační protokol fungující přes internet.
SRTP	Secure RTP. Zabezpečený protokol přenosu RTP toku.
SSH	Secure Shell. Síťový protokol pro zabezpečení datové komunikace.
SSL	Secure Sockets Layer. Zabezpečení komunikace šifrováním a autentizací.
TCP	Transmission Control Protocol. Nejpoužívanější protokol transportní vrstvy.
TDM	Time Division Multiplex. Dělení multiplexu dle časových rámců.
TLS	Transport Layer Security. Protokol sloužící pro šifrování signalizace.
UA	User Agent. Koncové zařízení v SIP infrastruktuře.
UAC	User Agent Client. Koncové zařízení v SIP infrastruktuře na straně klienta.
UAS	User Agent Server. Koncové zařízení v SIP infrastruktuře na straně serveru.
UDP	User Datagram Protocol. Protokol pro přenos datagramů v síti.
VOATM	Voice over Asynchronous Transfer Mode. Přenos hlasu přes ATM síť.
VOFR	Voice over Frame Relay. Přenos hlasu přes Frame Relay síť.
VOIP	Voice over Internet Protocol. Přenos hlasu prostřednictvím IP protokolu.
VPN	Virtual Private Network. Virtuální privátní síť.
WEBRTC	Web Real-Time Communication. Podpora tel. hovorů, videa přes prohlížeč.
XMPP	Extensible Messaging and Prevence Protocol. Protokol pro posílaní zpráv.
XML	Extensible Markup Language. Značkovací jazyk.

Úvod

IP telefonie platí v dnešní době, kdy svět kráčí směrem digitalizace a postupné internetové globalizace napříč sférami všech kategorií, za velice vyhledávané řešení na poli telekomunikací. Ačkoli se IT trendy velmi rychle mění a technologie se neustále zdokonalují, IP telefonie se těší stále narůstající oblibě s otevřenou budoucností. Tento způsob komunikace lze využívat skrze mobilní telefony, počítače, stolní telefony, tablety atd.

Podrobněji je zmiňovaná technologie charakterizována v první kapitole, ve které je definován pojem „IP Telefonie“ a všechny segmenty úzce spjaté s danou tematikou, jako jsou stavební prvky VoIP infrastruktury, využívané standardy, přenosové koncepty apod. V další části kapitoly jsou představeny možnosti emulace jednotlivých prvků v podobě koncových bodů, SIP serverů a ve finále kompletních IP telefonních modelů. Emulací je v tomto případě myšleno nakonfigurování navržených topologií za pomocí jiných nástrojů než těch defaultně určených. Úlohu emulace plní softwarový nástroj GNS3, který byl zvolen díky své celkové kompatibilnosti a budoucí možné snadné rozšiřitelnosti navrhnutých topologií. V závěru této kapitoly je popsáno toto emulačního prostředí, tj. jeho instalace, uživatelský manuál, důležité součásti, funkční bloky.

Tímto se práce dostává k jádru svého primárního určení představujíce navrhnutí IP telefonních modelů způsobem pokrývajícím všechny dostupné varianty emulace a možností demonstrace, co možná největšího spektra rozšířených funkcí dnešních IP telekomunikací. To vše za využití populárních softwarových aplikací typu Asterisk, Elastix, Kamailio, nesčetného množství SIP klientů a dalších potřebných programů. Kupříkladu Asterisk je často definován jako jedno z „nejsilnějších“ flexibilních, rozšiřitelných řešení v oblasti integrovaného telekomunikačního softwaru.

Druhá kapitola této práce je věnována právě návrhu jednotlivých modelů, kdy jsou popsány jejich základní vlastnosti, uplatněný software, předpoklady pro využití a schéma funkčnosti. Logicky navazuje konfigurace spjatá s použitými zdrojovými kódy, dokumentovanými kroky postupné implementace a problémy, které se mohou při sestavování naskytnout. Po úspěšném dokončení musí být podniknuty testovací cykly, kdy je potřeba odstranit případné komplikace, tak jako u každého nového „produktu“. Těmto procesům a samotným dílčím testováním přidružených specifických funkcí jsou podrobeny kapitoly s číslem tři a čtyři.

Závěr této diplomové práce spočívá v přizpůsobení vyhotovených modelů, a to tak, že jsou některé jejich části cíleně vymazány. Především jde o smazání nastavení softwarových klientů, a to s tím účelem, aby si tyto chybějící bloky implementace studenti mohli následně doplnit v rámci cvičení, ve kterých budou muset nejprve porozumět dané problematice. Rovněž bude vytvořena uživatelská dokumentace mapující tyto kroky. S nadsázkou lze říci, že bude navržena náplň jednoho či dvou cvičení předmětů, které se věnují IP telefonii.

1 IP telefonní infrastruktury

Infrastruktura bývá často označována jako kompozice všech složek v IT prostředí, přičemž těmito složkami mohou být hardware, software, síťové zdroje nebo další využívané služby. Kompozice určuje správnost jejich struktury, rozdělení, hierarchie tak, aby efektivně a účelně sloužily v daném prostředí.

1.1 IP telefonie

Tímto pojmem je označován mechanismus přenosu hlasu pomocí datových sítí, které jsou založeny na IP protokolu. Od toho také název IP telefonie, která bývá často označována zkratkou VoIP, což znamená přenos audiovizuálních záznamů v podobě IP paketů v rámci internetu a intranetových sítí. Využívá tzv. TCP/IP modelu, což je sada protokolů a pravidel, která definuje síťovou komunikaci.

Přenos hlasu přes IP sítě je založen na principu přepojování paketů. Lidský hlas je zachycen díky mikrofonu, za pomocí kodeků je konvertován do digitální podoby a poté je rozdělen do jednotlivých bloků, které prochází přenosovým médiem (fyzická vrstva). Jakmile tyto pakety dorazí k druhému účastníkovi, jsou opětovně poskládány a původní signál je zrekonstruován. Pro přenos jednoho slova je potřeba více datových bloků.

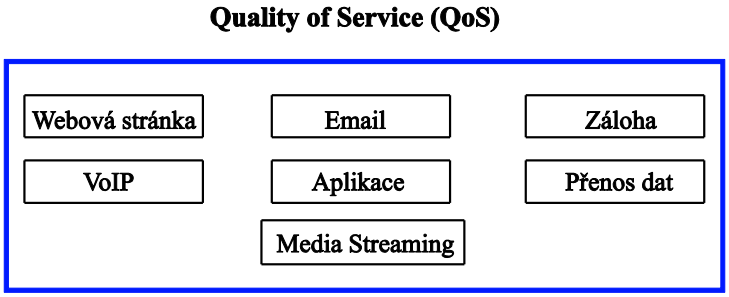
Poprvé byl tento způsob komunikace využit v roce 1995, kdy izraelská firma Volcatec prezentovala v USA svůj první „Internet Phone“. Tak vznikl tento standard, který je díky internetové dostupnosti využíván po celém světě ve většině firem, domácností, organizací.

Jedná se o lákavé telekomunikační řešení, jelikož tato alternativa je mnohem ekonomičtější než klasické PSTN (Public Switched Telephone Network) telefonování, neboť náklady na uskutečnění hovoru jsou prakticky zahrnuty v měsíčním paušálovém připojení k Internetu, které je dnes zavedeno téměř v každé domácnosti nebo firmě. Praktická využitelnost se dotýká především firem, v nichž je možnost propojit VoIP technologii s firemními systémy. Společnosti tak mohou využívat výhod vzdálené administrativy, konferenčních hovorů (audio i video), vybavenosti moderních IP telefonů, možnosti volání zdarma na firemní přístroje, zahraničních hovorů atd.

Mezi nevýhody IP telefonie bývá nejčastěji zařazována citlivost na odezvu sítě (tzv. latence). Tedy kolísání, respektive pravidelnost doručování, výpadky a zpomalení přenosu. Může tak docházet ke krácení přenášených paketů nebo k jejich nenávratnému ztracení. IP protokol často nebere ohled na to, která data by měla být upozaděna a která by naopak měla mít přednost. Proto je v IP telefonii kladen důraz na spolehlivost a rychlost přenosu. O to se starají definované standardy, jež jsou detailně popsané v následující podkapitole. Zde jsou pro přehled uvedeny všechny problémy, které se mohou objevit při návrhu a realizaci VoIP infrastruktury:

- **Zpoždění (Latence):** Je definováno jako časový rozdíl mezi dvěma okamžiky. Mezi vyslovením určitého slova do mikrofonu a jeho doručením k reprodukci na druhé straně (nebo naopak). Přijatelné zpoždění je stanoveno na hodnotu 150 ms.
- **Kolísání zpoždění (Jitter):** Jedná se o rozdíl mezi hodnotami zpoždění jednotlivých paketů. Pokud například paket číslo 1 dorazí se zpožděním 100 ms a paket číslo 2 se zpožděním 120 ms, jitter bude 20 ms.

- **Ozvěna:** Nastává, pokud uživatel slyší vlastní hlas v telefonním sluchátku. Existují systémy zajišťující potlačení tohoto negativního jevu. Například společnost Cisco ve svých hlasových bránách využívá systémů Extended Echo Canceler a Echo Suppressor.
- **Ztráta paketů:** VoIP sdílí přenosové médium s dalšími datovými službami, které mohou při své vysoké datové náročnosti omezovat samotnou IP telefonii. Může tak docházet k určitému „přehlcení“ a vytvoření fronty datových paketů, které mohou být v souvislosti s tím zahazovány, a pak dochází k sekání probíhajícího hovoru. Řešením je zavedení tzv. QoS, které se snaží zajistit vyhrazení a dělení dostupné přenosové kapacity tak, aby nedocházelo k zahlcení sítě.



Obrázek 1.1: QoS

1.1.1 Standardy pro VoIP

Jedná se o standardizované protokoly a principy, které IP telefonie využívá ke své funkčnosti. Jsou to nezbytné a důležité části této technologie. Tyto protokoly se primárně dělí na:

- Transportní
- Signalizační

Transportní

Protokoly, mající za úkol přenos paketů, se nazývají transportní. Řadí se sem především RTP a UDP. RTP jsou určeny pro práci s „hlasovými“ daty. Jsou tedy využívány při slovních konverzacích mezi dvěma a více volajícími stranami. Jinými slovy přenáší tzv. hlasový obsah. RTP je integrováno do UDP datagramu a strukturou se skládá z těchto položek:

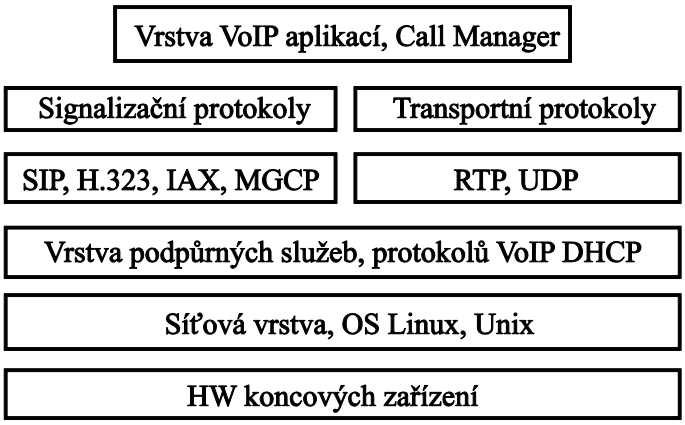
- **Payload type:** Tento parametr určuje typ transportovaného média. Základní profily jsou stanoveny v RFC 3551.
- **Sequence number:** Je to číslo identifikující paket o délce 16b.
- **Timestamp:** Využití např. ke zjištění parametrů jitter nebo zpoždění.

Data se přenášejí pomocí protokolu UDP fungujícího na portu 5060. Jeho primárním účelem je zajistit rychlou propustnost přenášených paketů přes síť. Dbá na doručení přicházejících dat v co nejkratším čase, ovšem nezaručuje spolehlivost, ani jejich správné doručované pořadí.

Signalizační

Mezi signalizační protokoly patří především H.323, SIP, IAX, MGCP a SCCP. Jejich primárním účelem je řízení relací, které se starají o navazování a ukončování spojení mezi dvěma a více koncovými body neboli klienty.

Novější a více známou variantou je protokol SIP. Ten je využíván i v této DP práci, a proto je rozveden v následující podkapitole. Za zmínku stojí ještě SDP, který zprostředkovává popis vlastností jednotlivých účastníků. Z komerční sféry pak protokol SCCP umožňující navázání komunikace na Cisco prvcích. Funguje na portu 2000/TCP a skladbou hlavičky je oproti SIP jednodušší. Hlas je i zde přenášen pomocí protokolu RTP.

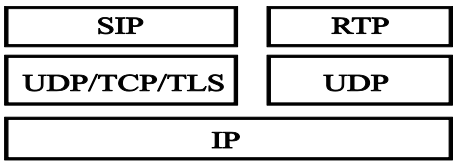


Obrázek 1.2: Model VoIP z hlediska OSI

1.1.2 **SIP**

Je textový protokol aplikační vrstvy podobný strukturou a principy například protokolům SMTP a HTTP. Tělo zprávy je utvořeno textovými položkami, které popisují předávané informace. Tyto položky jsou tvořeny znakovou sadou UTF-8, která umožňuje jednoduchou diagnostiku a zjišťování chyb bez speciálních analyzátorů.

SIP byl vytvořen organizací IETF jako IP standard, který sestavuje, modifikuje a ukončuje spojení mezi dvěma a více účastníky. Dle RFC 4566 nepřenáší SIP žádná data, nýbrž vyjednává a řídí parametry spojení.



Obrázek 1.3: Model protokolu SIP

Hlavní výhody SIP spočívají především v propojitelnosti mezi jednotlivými poskytovateli, jednodušším vývoji aplikací, fungování se stávajícími IP protokoly, migraci koncových účastníků. Nabízí také snadnější fungování přes firewall brány.

Prvky architektury SIP protokolu

Architektura protokolu SIP je založena na 5 částech, z nichž má každá komponenta svá specifická určení:

- **User Agent (UA):** Jde o koncová zařízení, většinou hardware nebo software telefon. Často je mezi ně zařazována i brána (Gateway). Terminál SIP UA se skládá ze dvou částí, a to User Agent Client (UAC) a User Agent Server (UAS). Všechny telefony, které využívají protokol SIP, musí obsahovat tyto dva zmiňované logické bloky. UAC je určen k zahájení inicializace spojení a UAS reaguje na žádosti a posílá odpovědi.

  Koncová zařízení jsou adresována pomocí dvou částí. První část slouží k určení uživatele např. 3004. Ta druhá, která je oddělena pomocí znaku „@“, pak poskytuje identifikaci hostitele domény. Ve finále může kompletní adresace koncového zařízení vypadat například takto: **„3004@192.168.1.4“**
- **Proxy server:** Zastupuje koncové zařízení při předávání požadavků na další server. Po získání adresy volaného účastníka sám naváže spojení a potvrdí jej volajícímu účastníkovi.
- **Redirect server:** Posílá zpět upozornění koncovému zařízení, že volaný účet je umístěn někde jinde. Poté zašle jeho novou polohu. Koncové zařízení nebo proxy server pak kontaktuje tuto adresu.
- **Register server:** Registruje jednotlivé uživatelské účty na základě jejich připojení do datové sítě a ukládá je do databáze aktuálního umístění koncového zařízení. Tyto informace zprostředkovává lokalizační službě a provádí aktualizaci všech zařízení v síti v rámci domény.
- **Location server:** Má přístup k Register serveru a odpovídá na dotazy týkající se umístění jednotlivých koncových zařízení [4], [5].

SIP zprávy

SIP je v dnešní době standard, který je podporován téměř ve všech hardwarových a softwarových VoIP telefonech. Funguje na koncepci klient-server, tudíž komunikace probíhá výměnou dvou typů zpráv, a to **požadavků** a **odpovědí**. Pod pojmem „klient“ si lze představit IP telefon nebo SW aplikaci a pojem „server“ značí aplikační server služeb. Požadavky jsou v jádru SIP protokolu rozděleny dle RFC 3261 do šesti následujících kategorií:

- **INVITE:** Slouží k pozvání uživatele nebo služby k podílení se na relaci. Tělo zprávy obsahuje popis relace (spojení).
- **ACK:** Potvrzení, že klient přijal zprávu INVITE a vstupuje do komunikace.
- **BYE:** Oznámení protistraně, že uživatel chce ukončit hovor. Metoda BYE může být vyslána jak volaným, tak volajícím.
- **CANCEL:** Vyjadřuje přerušení procesu zahájení relace ještě před jejím navázáním.
- **REGISTER:** Registruje současné adresy klientů u SIP serveru, který je předá lokalizační službě.
- **OPTIONS:** Je metoda pro zjištění vlastností SIP zařízení. Má podobnou strukturu jako požadavek INVITE.

Na každý vyslaný požadavek je potřeba také odpovědi, vyjma požadavku ACK. Odpovědi jsou v rozsahu 100 až 699 a jsou následující:

- **1xx:** Prozatímní odpovědi typu požadavek přijat, vyzvání atd.
- **2xx:** Úspěch. Požadavek je přijat, pochopen a akceptován.
- **3xx:** Přesměrování. Je třeba vytvořit nový upravený požadavek.
- **4xx:** Chyba klienta. Špatná syntaxe požadavku, nebo požadavek nemůže být proveden.
- **5xx:** Chyba serveru. Server není schopen provést platný požadavek.
- **6xx:** Globální chyba. Požadavek nelze provést.

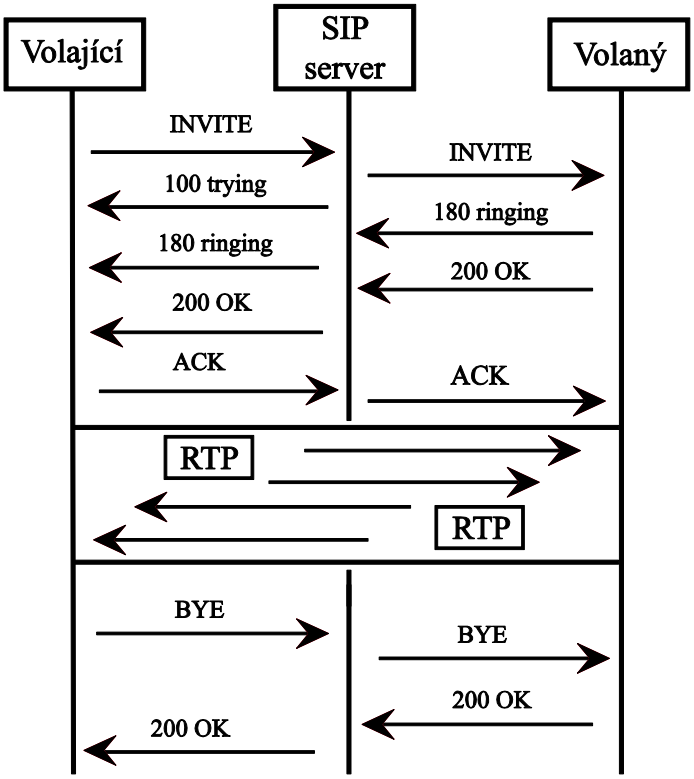
Zde je vložena typická hlavička signalizace SIP protokolu. Popis nejdůležitějších parametrů se nachází pod obrázkem.

```
INVITE  sip:7170@iptel.org   SIP / 2.0
Via: SIP / 2.0 / UDP 195.37.77.100:5060
Max- Forwards: 10
From: „richard“  <sip:richard@iptel.org>tag=76ff7a07-c091-4192-84a0d56e91fel04f
To: <sip:richard@bat.iptel.org>
Call- ID: d10815e0-bf17-4afa-8412-d9130a793d96@213.20.128.35
CSeq: 2 INVITE
Contact: <sip:213.20.128.35:9315>
User-Agent: Windows RTC / 1.0
Proxy-Authorization: Digest username= „richard“, realm=„iptel.org“,
algorithm=„MD5“, uri=„sip:richard@bat.iptel.org“, nonce =
„3cef753800000001771328f5ae1b8b7f0d742da1feb5753c
```

Obrázek 1.4: Hlavička protokolu SIP

- **Call ID:** Označuje identické číslo hovoru. To je vygenerováno náhodně klientem pro každý směr. Po dobu probíhajícího spojení se nemění.
- **Contact:** Obsahuje SIP adresu, pomocí které lze navázat spojení s volaným bez nutnosti použití Redirect serveru.
- **CSeq:** Pořadové číslo žádosti v rámci jednoho hovoru. Číslo se zvyšuje zasláním nového požadavku INVITE.
- **From:** Jedná se o adresu, ze které uskutečňuje hovor volající.
- **To:** Tento parametr určuje IP adresu volaného.
- **Via:** Do tohoto parametru Proxy server vkládá svoji adresu. Při odesílání druhým, opačným směrem, ji odstraní. Zabraňuje tak vzniku smyček.

Hlavní výhodou protokolu SIP je jeho jednoduchost. Navazování spojení je navíc velmi rychlé. Právě proto dnes většina VoIP zařízení využívá standard SIP. Ukázku toho, jak probíhá sestavení spojení mezi dvěma účastníky, demonstruje obrázek na následující straně.



Obrázek 1.5: Ukázka SIP signalizace

1.1.3 Kodek

Ovlivňuje kvalitu spojení a nároky na internetové připojení. Jeho primárním úkolem je co nejvěrněji a v co možná nejlepší kvalitě převést vstupní signál, což je většinou lidský hlas, zachycený mikrofonem. Signál je převáděn do digitální podoby, a to takovým způsobem, aby zabral co nejméně přenosového pásma. Zde jsou uvedeny některé příklady telekomunikačních kodeků:

- **G.711:** Základní kodek veřejné telefonní sítě. Tento standard digitalizuje hlas do 64 Kbps a nekompresuje ho.
- **G.722:** Funguje na 64 Kbps, nabízí vysokou kvalitu hovoru.
- **G.723:** Jednalo se o doporučovaný standard pro kompresi. Funguje na 5,3 a 6,3 Kbps. Není příliš populární v oblasti VoIP a je považován za horší než standard G.729.
- **G.726:** Poskytuje téměř stejnou kvalitu jako G.711, zabere však jen poloviční šířku pásma.
- **G.729:** Úsporný hlasový kodek.
- **H.263, H.264:** Videokodeky používané např. při videokonferencích.

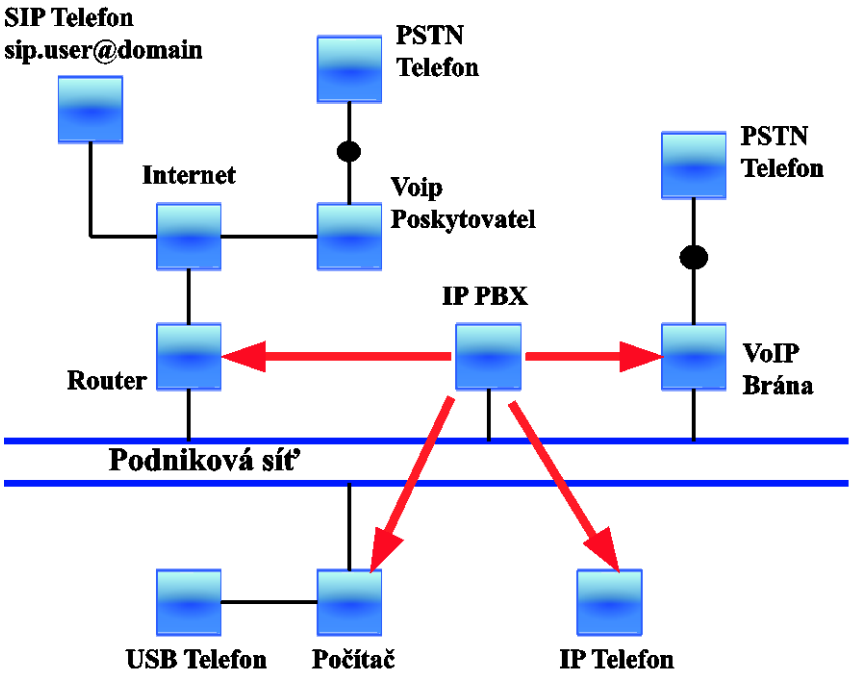
1.1.4 VOIP telefonní infrastruktury

V této podkapitole je uvedena jedna konkrétní struktura VoIP v praxi. Především z důvodu zprostředkování lepší představy o tom, jak je možné prvky telekomunikačních sítí příkladně zakomponovat do jedné infrastruktury, která může usnadňovat práci lidem v dané společnosti.

Na obrázku se nachází server IP PBX (ústředna), jenž je integrován v telefonní síti. Lze si

povšimnout, že funguje jako propojovací bod mezi jednotlivými „světy“.

Základ infrastruktury tvoří firemní síť, která zahrnuje koncová zařízení typu IP Phone, USB Phone atd. Část popisované infrastruktury se skládá z veřejné telefonní sítě (PSTN). Ta je integrována do celku pomocí tzv. brány. Přes internet jsou poté připojeni SIP klienti a pomocí providera další PSTN linky.



Obrázek č. 1.6: Ukázka firemní VoIP infrastruktury

Komplexnost VoIP infrastruktur může být opravdu obrovská a záleží pouze na počátečním návrhu dané topologie. Ten by se měl odvíjet od toho, jak je potřeba danou síť poskládat pro konkrétní účely, jaké množství prvků bude využito, kolik je schopen tazatel investovat do sítě apod. Samozřejmě to vše také s ohledem na bezproblémovou funkčnost.

SIP servery

Telefonní ústředna je zařízení, ke kterému jsou připojeny telefony nebo další ústředny. Primárním účelem ústředny je spojování hovorů mezi jednotlivými telefony. Dělí se na hardwarové a softwarové.

Zde není potřeba detailně charakterizovat hardwarové ústředny ani jejich případné dělení. Postačí uvést, že ústředny jsou označovány zkratkou PBX a v případě této práce bude využito hlavně ústředen softwarových, které jsou často jednotlivě označovány pojmem SIP server. Mezi nejznámější patří Asterisk, CUCME (Cisco), Elastix, Kamailio.

Koncová zařízení

Jak už z názvu plyne, jedná se o zařízení nacházející se na koncových uzlech VoIP telefonní sítě. Jejich rozdělení je následující:

- VoIP brána
- Hardwarový telefon
- Softwarový telefon

VoIP brána

Zajišťuje konverzi hlasové komunikace mezi jednotlivými sítěmi. Převod může probíhat mezi analogovou, digitální a VoIP telefonií. Uživatelé bránu nejčastěji využívají tak, že „propojí“ svůj analogový telefon s VoIP bránou (Gateway).

Brána může být realizována jako samostatné zařízení nebo jako součást jiného celku, např. směrovače, telefonní ústředny nebo serveru. Je často zařazována mezi koncová zařízení.

Hardwarový telefon

Jde o fyzické zařízení, které je dostupné ve stolní nebo částečně bezdrátové variantě. Vzhledem je téměř nerozeznatelné od klasických analogových telefonů. VoIP telefony jsou však o něco chytřejší. Jde v podstatě o jednoúčelové počítače, na kterých běží jejich vlastní softwarový telefon. Stejně jako počítače mají telefony napevno přidělenou statickou nebo pomocí DHCP serveru dynamickou IP adresu. Většina přístrojů je vybavena konektorem RJ45 pro ethernetový kabel, kterým se připojují do IP sítě. Telefony obsahují gigabitový port a některé mají tzv. miniswitch, což je síťový přepínač, který slouží k zapojení dvou zařízení do datové přípojky pomocí jednoho kabelu.

Tato zařízení mají velké množství funkcí, které jsou k využití jak ve firemním, tak domácím prostředí a podporují hlavně standardy SIP a SPCP. Hardwarový telefon je většinou nastaven pomocí operátora, u kterého je zakoupen. Případně je v rámci koupě přibalen kompletní manuál s dostupnou online podporou. Pro představu jsou na obrázku 1.7 ilustrovány HW telefony, které jsou na dnešním trhu (2017) nabízeny.

Obrázek 1.7: Druhy hardwarových telefonů

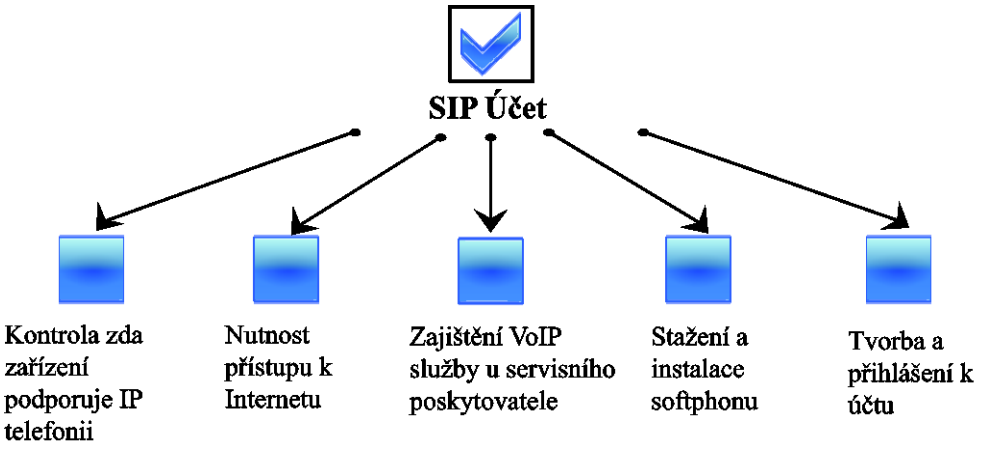
Softwarový telefon

Prakticky jde o program, který si uživatel stáhne do svého počítače, mobilu, tabletu a po jeho úspěšné instalaci si musí založit profil s přihlašovacími údaji. Pod tímto profilem nadále vystupuje a je mu umožněno navazovat případná spojení s jinými uživateli.

Jedná se tedy o nejdostupnější možnost VoIP komunikace. Software je potřeba si nastavit

většinou vlastním umem. Nastavuje se číslo účtu, doména, využívaný port atd. Nebývá to ovšem složité a na internetu existuje mnoho návodů. Poté je potřeba mít jen mikrofon a případně sluchátka nebo reproduktory.

Existuje spousta softwarových telefonů, ať už těch volně přístupných či placených. Jejich seznam a přehled je dostupný ve zdrojích [17]. Mezi lidově nejrozšířenější patří např. Skype, X-Lite, Yate.



Obrázek 1.8: Cesta k SIP účtu

V následující podkapitole bude věnována pozornost emulačnímu nástroji GNS3, který bude posléze využíván při realizaci navržených topologií.

Proces emulace je definován jako napodobování chodu programu nebo zařízení na prostředcích, neodpovídajících přesné technické specifikaci napodobovaného zařízení [3]. Emulace může být také chápána jako případ virtualizace.

1.2 GNS3

Je to open-source grafický simulátor sítí, který umožňuje emulovat především síťové prvky. Ovšem lze do něj „vložit“ i prvky z telefonní infrastruktury. V programu se tedy mohou utvářet komplexní topologie, na kterých je poté možno provádět určité testování funkčnosti, předpřipravit si tak konfiguraci reálné sítě, využít je k výuce apod. Jádrem nástroje GNS3 je program Dynamips, který tyto emulace umožnuje. GNS3 je tudíž grafická a uživatelsky mnohem přívětivější verze zmiňovaného programu, fungující na platformách Windows, Linux a MacOS X.

V podstatě se jedná o virtualizační vrstvu, která simuluje HW konkrétních komunikačních zařízení. Jedná se především o síťová zařízení firem Cisco a Juniper. V případě společnosti Cisco bývá často také skloňován pracovní název Cisco IOS. Prostředí GNS je rovněž schopno pracovat i s virtuálními stroji, které byly předem vytvořeny programy VirtualBox či VMWare. Ty jdou poté snadno do tohoto simulačního prostředí naimplementovat. Na tento fakt bude navázáno v kapitole dvě zabývající se návrhem IP emulačních telefonních modelů [1].

K provedení celkových komplexních simulací využívá GNS i další programy, které rozšiřují paletu funkcí. Patří mezi ně především Qemu, Putty, Wireshark, Dynagen atd. Jejich seznam a přehled je uveden níže.

Na podporu GNS3 vznikly v roce 2014 zcela nové stránky včetně uživatelského fóra, kde lze diskutovat s jinými uživateli, získat cenné rady nebo tutoriály k uživatelskému použití. Také je zde možnost si bezplatně stáhnout tento software v aktuální verzi. Ke správné neomezené funkčnosti a možnosti pracovat s velkým množstvím zařízení je zapotřebí být vlastníkem Cisco IOS obrazů, které se nahrávají do programu. Přitom je dobré pamatovat na to, že emulovaná zařízení mají hardwarové nároky, stejně jako zařízení reálná, tudíž jejich navyšující se počet posléze značně vytěžuje danou PC sestavu. Je nutné myslet i na dostupný výkon PC zejména RAM a procesoru.

Dnešní download balíček obsahuje všechny nápomocné níže zmíněné programy včetně GNS3, ovšem pouze s defaultními IOS obrazy. Pokud chce mít uživatel „rozšířenou“ verzi obsahující větší výběr mezi emulovanými prvky, je nucen zakoupit jejich IOS obrazy [2].

Obrázek 1.9: GNS3 logo

Přehled nápomocných programů:

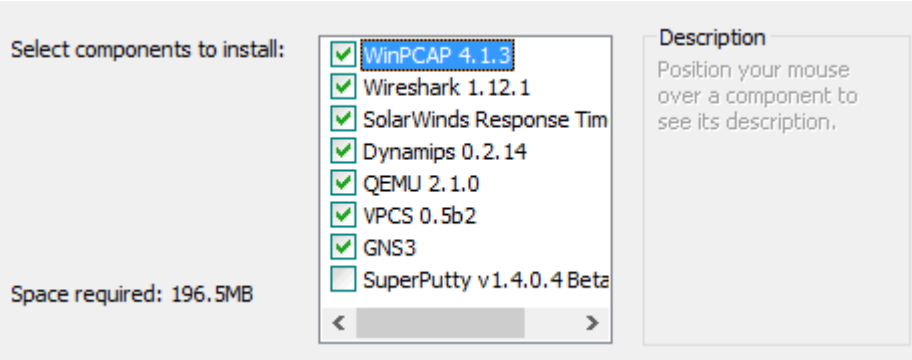
- **Dynamips:** jádro pro emulování Cisco směrovačů
- **Dynagen:** textové rozhraní pro Dynamips
- **Qemu:** generický emulátor a virtualizační nástroj pro spuštění virtuálních strojů
- **Putty:** telnet, SSH klient, slouží k připojení na konzole virtuálních zařízení
- **Wireshark:** nástroj pro zachytávání a analýzu síťového provozu, umožňuje prohlížet a analyzovat tato data
- **WinPCAP:** umožňuje síťové kartě fungovat v hybridním módu
- **Pemu:** určitá varianta Qemu, která je využívaná v rámci PIX firewallů

Shrnutí jednotlivých funkcí programu GNS3:

- návrh komplexních síťových topologií
- emulování směrovačů platformy Cisco IOS, IPS, PIX a ASA firewally, JunOS
- simulace jednoduchých Ethernetových, ATM a Frame relay přepínačů
- zachytávání paketů a jejich analýza v programu Wireshark
- propojení simulační části do skutečné sítě

1.2.1 Instalace

Nejjednodušší cestou je stažení balíčku „All in one“, který obsahuje všechny potřebné výše zmíněné programy. Je zcela na uživateli, kterými částmi se rozhodne své GNS doplnit. Nejvhodnější je ponechat vše zatržené (viz obrázek 1.10). Velikost balíčku je přibližně 60 MB, obsahuje instalátor pro 32 bitové a 64 bitové operační systémy.



Obrázek 1.10: Volba programů k instalaci

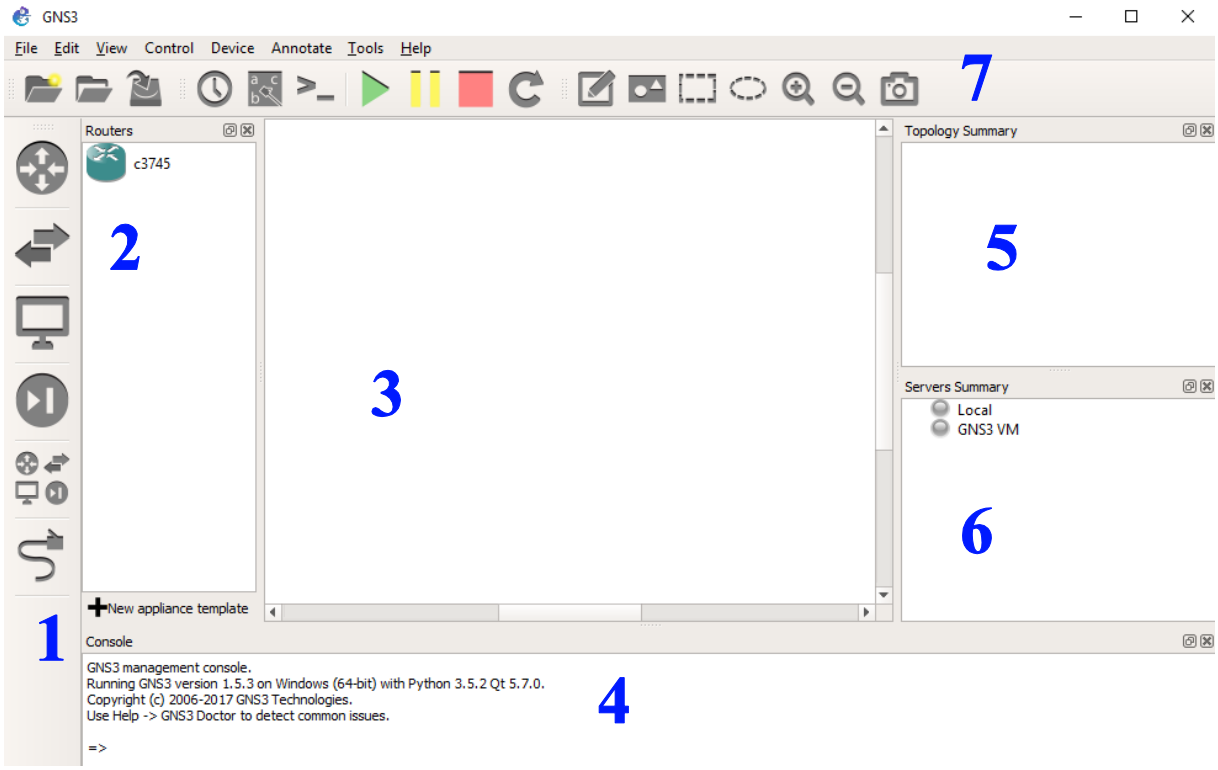
Po úspěšné instalaci již lze program GNS3 spustit. Při naběhnutí je uživatel dotázán na připojení GNS3 k virtuální vrstvě. Je možno využít VMWare, VirtualBox či lokální server.

Je důležité vytvořit potřebné virtuální stroje a nastavit jim dané povolené využití RAM. To by mělo být nastaveno, s ohledem na výkonnostní parametry, uživatelem využívaného stroje. Poslední krok představuje přidání stažených IOS obrazů do GNS3. To by byla ve zkratce instalace.

Jelikož je velice dobře popsána jak v originálním tutoriálu [8], [9], který je dostupný na stránkách softwaru, tak při instalaci samotné, není třeba se této části více věnovat. Nyní je možno přejít k obsluze samotného programu.

1.2.2 Obsluha programu

Grafické uživatelské rozhraní GNS3 demonstruje ilustrace 1.11, jež je rozdělena do několika kategorií, jejichž význam a primární určení jsou popsány pod obrázkem.



Obrázek 1.11: Uživatelské rozhraní GNS3

1) Levý pás ikon: jedná se o ikony síťových prvků, které jsou ustanoveny dle dohodnutých pravidel. Jde především o routery, switche a všechny další dostupné síťové prvky potřebné pro vytvoření dané topologie.

2) Rozšíření levého pásu ikon: při výběru konkrétního síťového prvku se otevře další pás, kde jsou již specifická zařízení daného prvku, pro které je nainstalován IOS obraz.

3) Pracovní plocha: zde lze utvářet konkrétní topologie pomocí přetažení a spojování daných prvků z předchozích dvou popsaných oken. Je možno vidět daný stav vybraného rozhraní, zda je aktivní či neaktivní.

4) Konzole Dynagenu: jedná se o textový vstup a výstup programu Dynamips. Poskytuje jednotlivé výpisy o stavu zmiňovaného programu a jeho rozběhnutých procesech.

5) Zachycený provoz v dané topologii (síti)

6) Sumarizace všech prvků umístěných na pracovní ploše: popis rozhraní, stanovení místa, kde jsou napojena, zobrazení jejich stavu atd.

7) Lišta řídících operací: zde je potřeba detailnějšího popisu nacházejícího se níže.

Obrázek 1.12: Lišta operací

a)	Založení nového projektu, stačí zvolit pouze název a lokalitu uložení.
b)	Otvírá již uložené projekty.
c)	Slouží k rychlému uložení stávajícího projektu.
d)	Umožňuje vytvářet obrazy aktivní topologie a její konfigurace, určeno k dokumentaci postupu, obsahuje čas pořízení atd.
e)	Odkrývá/skrývá popis portů a jednotlivých zařízení.
f)	Propojení všech konzolových zařízení.
g)	Spouští nebo probouzí ze spánku celou konfiguraci (topologii).
h)	Slouží k pozastavení funkčnosti topologie (running config není smazán).
ch)	Zastaví celou topologii (runnig config je smazán).
i)	Funguje jako restart, veškeré procesy se rebootují a spustí se znovu.
j)	Tímto lze vložit libovolnou poznámku.
k)	Vložení obrázku.
l)	Vložení obdélníku do pracovní plochy.
m)	Vložení elipsy do pracovní plochy (lze tak ohraničit a oddělit od sebe jednotlivé části topologie).
n)	Slouží k přiblížení daného bodu, pokud je potřeba.
o)	Oddaluje.
p)	Slouží k aktuálnímu pořízení fotky toho, co je zrovna na pracovní ploše.

1.2.3 Základní síťové hardwarové prvky

Jedná se o základní síťové hardwarové prvky, které je možno emulovat v softwaru GNS3. Zde je naznačen primární účel jejich využití a částečný přehled vnitřního nastavení.

a) Router (Směrovač)

b) Switch (Síťový přepínač)

c) End Devices (Koncové zařízení)

d) Security Devices (Bezpečnostní zařízení)

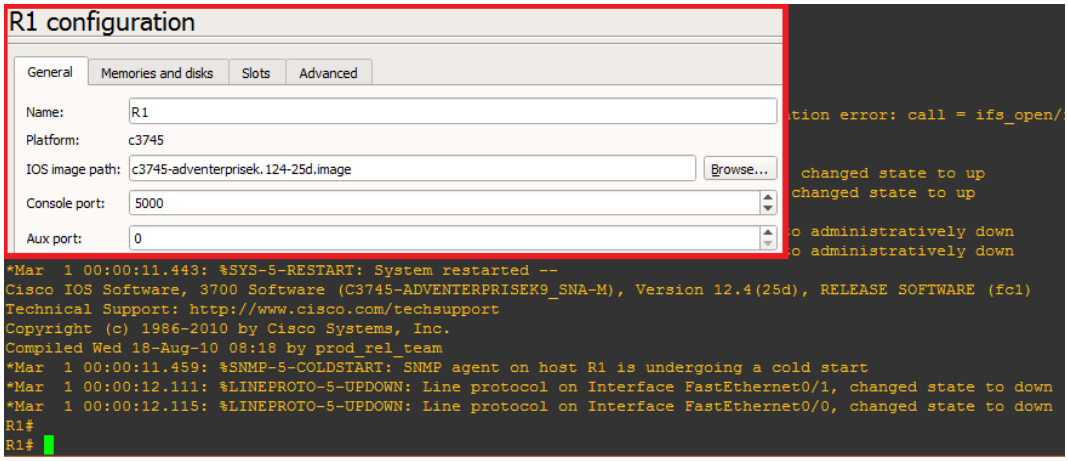
e) All Devices (Výběr všech zařízení)

f) Link (Propojovací kabely)

Router

Nazývaný také často jako směrovač, je síťové zařízení využívané především v počítačových sítích. Jeho primárním účelem je přeposílání datových paketů směrem k cíli. Lze jej definovat jako „hraniční přechod“ mezi jednotlivými sítěmi. Router se v GNS3 značí pomocí symbolu, viz předchozí obrázek a).

V programu je umožněno zvolit jen ty routery, které mají naistalován IOS odpovídající verze. Pro dané specifikace je nutné rozkliknout prvek routeru na pracovní ploše. Následně se zobrazí obecný popis zařízení, který je rozdělen do několika záložek. Je možno sledovat porty a velikost přidělené RAM, připojovat adaptéry na volné sloty atd. Spuštění směrovače se provádí pokynem START. Nejdůležitější volbou je ovšem položka terminálu, přes který je pomocí příkazů zpřístupněna konfigurace funkčnosti daného zařízení. Tuto akci lze provádět až po spuštění routeru a spouští se pokynem CONSOLE. Mezi terminály patří např. Putty, SuperPutty, Telnet. Dílčí seznam a základní popis použitelných IOS obrazů viz zdroje [16].



Obrázek 1.13: Základní informační přehled routeru (vlevo) a ukázka terminálu

Switch

Tento prvek sítě je často nazýván jako „chytrý směrovač“, který posílá pakety jen určeným příjemcům. Řadí se mezi aktivní síťové prvky a propojuje jednotlivá zařízení v síti.

Zařízení funguje tak, že kontroluje adresu uživatele a příjemce, která je obsažena v přenášeném datovém paketu a díky tomu přepíná pakety pouze na port, kde se cílové zařízení nachází. Tím také dochází k odlehčení ostatních portů. Switch je inovativní verze Hubu (rozbočovače), který data pouze kopíroval na všechny dostupné porty.

End Devices

Jedná se o koncová zařízení připojená k síti. Většinou jde o uživatelská PC, terminály, softwarové telefony atd. Je zde možnost připojit tzv. Cloud, což je „síťový mrak“, který zastupuje externí sítě.

1.2.4 Optimalizace

Pokud chce uživatel vytvářet komplexnější topologie, to značí více zařízení zapojených navzájem v síti, je vhodné zde uvést nástroje umožňující efektivní využití výpočetních zdrojů. Mezi tyto funkce patří v GNS3 především Ghost IOS, Sparemem, Mmap.

Pro fungování Ghost IOS a Sparemem je potřeba mít zapnutou funkci Mmap, která představuje základní kámen těchto dvou funkcí. Existuje ještě funkce Idle PC, která se stará o efektivní využití procesoru.

Všechny tyto nástroje jsou integrovány do prostředí GNS3. Bez nich by došlo velmi rychle k přetížení fyzické i virtuální paměti stroje, přičemž by aktuální využití RAM i procesoru dosahovalo velmi vysokých hodnot vytížení.

Idle PC

Dynamips je v podstatě emulátor, který provádí načítaní každé instrukce z binárního obrazu strojového kódu, a tu okamžitě uskutečňuje na hostitelském počítači. Tento proces se neustále opakuje. Proto je potřeba mít funkci vymezující smyčku, při níž budou provedeny všechny instrukce. Tudíž se nebudou opakovat neustále znova, ale jen jednou za daný čas. Touto zmiňovanou funkcí je Idle PC, která je schopna znatelně snížit vytížení CPU počítače a přitom „nezmrazit“ daný směrovač. Ten může díky tomu provést procesy, které potřebuje. GNS samo po dané kalkulaci nabídne seznam doporučených Idle PC hodnot, které je potřeba nastavit.

Ghost IOS

Může snížit využití fyzické paměti PC, pokud se pracuje se zařízeními, která využívají stejný IOS obraz. Aby si každý router neuchovával obraz ve své virtuální RAM paměti, počítač, na němž se emuluje zařízení, alokuje jednu sdílenou oblast paměti, kterou budou posléze všechna tato zařízení využívat.

Pokud by síť například obsahovala 7 zařízení se stejným operačním systémem a jeden IOS by představoval 30 MB, bez Ghost IOS by bylo obsazeno 210 MB paměti. Při zapnutí Ghost IOS ovšem zaplní jen 30 MB paměti počítače.

Sparesmem

Jedná se o funkci, která nešetří reálnou RAM paměť hostitelského PC. Namísto toho snižuje množství virtuální paměti používané emulovaným routerem. Tato funkce je důležitá také z pohledu OS, kdy např. 32 bitový Windows limituje jeden proces na 2 GB virtuální paměti. Pokud se tedy spustí tato funkce, dojde k alokaci pouze virtuální paměti, která je aktuálně využívaná operačním systémem směrovače v dané instanci. Nikoliv však pro celou nakonfigurovanou paměť.

Mmap

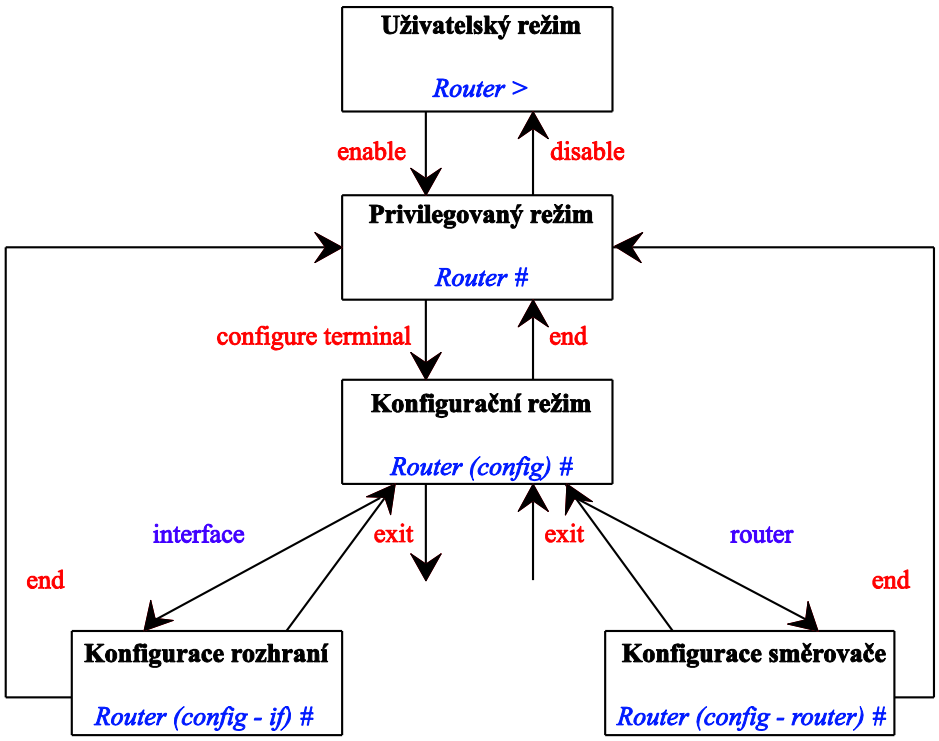
Vynucuje, aby Dynamips využíval stránkovací paměť, oproti paměti fyzické, pro instanci směrovačů.

1.2.5 Cisco IOS

Je to balík směrovacích, přepínacích a telekomunikačních funkcí od společnosti Cisco. Tento software je možno najít v zařízeních typu router, a dokonce i switch. To proto, že v dnešní době moderní přepínače obsahují i některé funkce, které byly v minulosti určeny jen pro směrovač.

Rozhraní

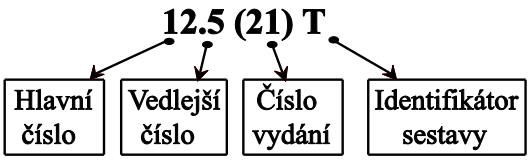
Umožňuje uživateli provádět konfiguraci zařízení. Rozhraní, které to umožňuje, se nazývá CLI a je rozděleno do několika režimů. V každém režimu je přístupná jiná sada příkazů s konkrétními uživatelskými právy. To adekvátně znázorňuje následující obrázek s názvem model režimů IOS.



Obrázek 1.14: Model režimů IOS

Verze

Jednotlivé verze se od sebe odlišují díky označení. To je provedeno pomocí čísel a někdy také malých písmen. Základní přehled a jejich dělení je demonstrováno na následujícím obrázku.



Obrázek 1.15: Identifikace verzí IOS

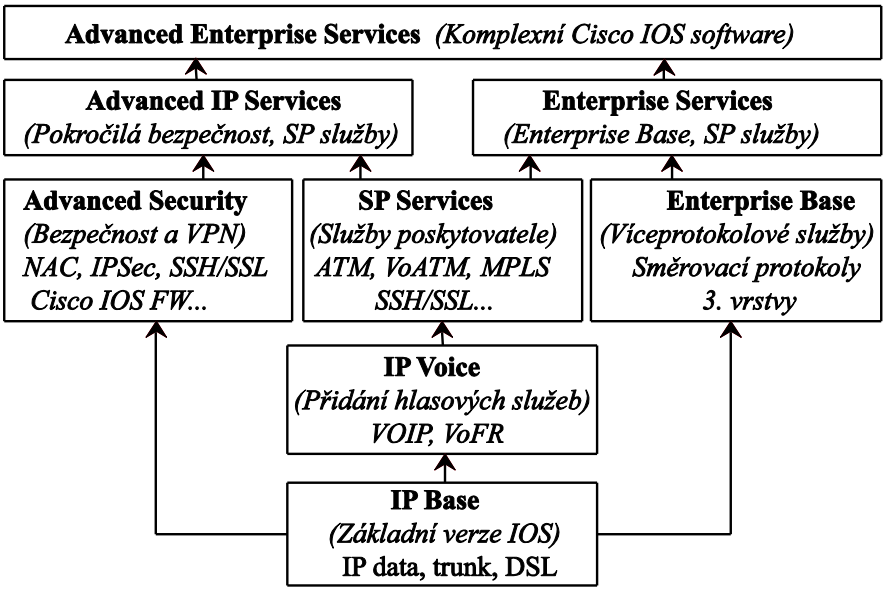
- **Identifikátor sestavy:** určuje, jak je daná sestava naladěna. Zda jde o základní verzi, nebo verzi, která je zaměřená (upravená) určitým směrem, např. pro jádro nebo podnikové sítě.

Balíčky

Spadají do kategorie služeb. Jsou to v podstatě specifické sady, příčemž každá má své konkrétní určení a funkce pro oblast vybranou ze všech oblastí zahrnujících nabízené síťové technologie. Mezi zástupce se můžou řadit např. služby pro poskytovatele, bezpečnost atd.

Hlavní myšlenkou zavedení jednotlivých balíčků bylo umožnit snadnější volbu správného softwaru. Dalším důvodem bylo vyhnout se vytvoření verze obsahující nadbytečné funkce, které by uživatel nevyužil. Jak si uživatel dané balíčky poskládá, je tedy jeho individuální volbou.

Jednotlivé části na sebe mohou navazovat, což lze vidět na obrázku 1.16.



Obrázek 1.16: Schéma IOS balíčků

- **Advanced Enterprise Services:** Je to plná verze Cisco IOS. Propojuje Advanced IP Services a Enterprise Services.
- **Advanced IP Services:** Jedná se o podporu pro IPv6, komplexní bezpečnost pro SP Services.
- **Advanced Security:** Pod tento balíček spadá Cisco IOS Firewall, IDS/IDP, NAC, SSH/SSL, IPsec a další.
- **Enterprise Base:** Zahrnuje směrovací protokoly 3. vrstvy ISO OSI.
- **Enterprise Services:** Podpora služeb pro IBM. Sloučení SP Services a Enterprise Base.
- **IP Base:** IP datová komunikace, trunk a DSL.
- **IP Voice:** Zahrnuje hlavně VoIP, VoFR.
- **SP Services:** Shlukuje komunikační služby SSH/SSL, ATM, VoATM atd.

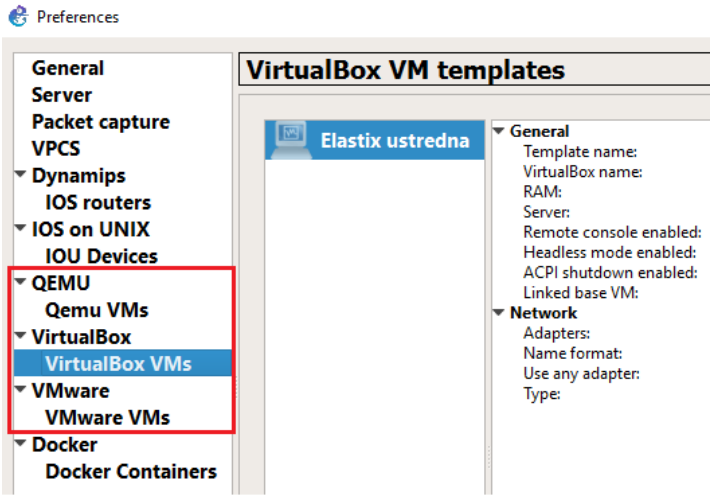
1.2.6 Virtualizace

Podstatou virtualizace je vytvoření virtuálního neboli „zdánlivého“ počítače uvnitř počítače fyzického, pomocí vhodného softwaru.

Dnes jde o velmi inovativní IT odvětví. Virtualizace se aplikuje k lepšímu využití existujícího hardwaru, ke konsolidaci a lepší implementaci nových serverů, k zálohování a migraci nebo vývoji softwaru. Dále se využívá také k otestování neznámých programů před tím, než se uživatel rozhodne je instalovat do svého PC atd.

V případě této diplomové práce bude k dílčím virtualizacím využito nástroje Virtualbox, ve kterém budou vytvořeny obrazy jednotlivých VoIP prvků. Ty jsou posléze naimportovány do emulačního prostředí GNS3 umožňujícího jejich spojení do jedné síťové virtuální telefonní infrastruktury, která bude otevřena možnostem dalšího rozšiřování dle uvážení. Může se jednat například o propojení více SIP serverů pomocí trunku apod.

Jak již bylo řečeno, GNS3 nabízí možnost naimportovat do svého uživatelského prostředí virtuální přístroje typu VirtualBox, VMware, QEMU a tímto je využít jako součást vytvářené cílové topologie. Proces se provádí pomocí záložky „Edit“ a následné volby „Preferences“, přičemž se otevře uživatelské okno zobrazené na obrázku 1.17. Poté již stačí jen zkompletovat topologii a započít proces její emulace.



Obrázek 1.17: Import virtuálních strojů do prostředí GNS

1.3 Emulované aplikace a systémy IP telefonie

Zde je popsán vybraný software, který byl využit ke tvorbě a emulaci navrhnutých modelů z následující kapitoly. V tomto případě jde o softwarové SIP servery a koncová klientská zařízení.

1.3.1 Asterisk

Jedná se o open source řešení pobočkové ústředny, které umožňuje realizovat IP telefonii, digitální ISDN i analogovou telefonii. Tato softwarová PBX běží na platformách Unixu a Linuxu. Asterisk byl vytvořen firmou Digium a oficiálně je definován jako open-source hybrid TDM a packet voice PBX. Vytváří rozhraní telefonnímu hardwaru, softwaru a libovolné telefonní aplikaci. Oblíbenost si získal díky své univerzálnosti a sice tím, že dokáže spolupracovat skoro s každým standardizovaným telefonním vybavením. Je schopen nahradit komunikační systémy renomovaných výrobců a stále jde o bezplatně dostupný software. Kromě klasických vlastností, kterými disponuje každá ústředna, se může pochlubit následujícími funkcemi:

- Různorodá VoIP gateway (MGCP, SIP, IAX, H.323)
- Pobočková ústředna (PBX)
- Voicemail služby s adresářem
- Interaktivní hlasový průvodce (IVR) server
- Softwarová ústředna (Softswitch)
- Konferenční server
- Packet voice server
- Šifrování telefonních nebo faxových volání
- Překlad čísel
- Aplikace Calling card
- Prediktivní volič (Predictive dialer)
- Řazení volání do front se vzdáleným zprostředkovatelem
- Vzdálené „kanceláře“ pro existující PBX

1.3.2 Elastix

Je moderní řešení kombinující open source PBX a pokročilý webový interface FreePBX. Při původním záměru vznikal Elastix jako webové rozhraní pro Asterisk. Dnes se jedná o uživatelsky méně náročnou verzi softwarového telekomunikačního serveru, který přináší funkce IP PBX, email serveru, fax serveru, instant messaging serveru (XMPP) apod. Jde o Linux distribuci virtuální VoIP ústředny s webovým rozhraním, která si klade za cíl zahrnout všechny komunikační alternativy a mít je stále k dispozici na podnikové úrovni v jednoduchém řešení. Mezi zajímavosti patří např. integrovaný kalendář s podporou Text to Speech, přičemž k uživatelem nastavené události může ústředna volat na upozornění.

1.3.3 Kamailio

Představuje open source SIP server, který byl vydán pod licencí GPL. Je napsán v jazyku C a primárně určen pro Unix a Linux systémy. Jeho výhodou je malá hardwarová náročnost a orientace na co možná nejvyšší poskytovaný výkon. Kamailio zahrnuje pouze potřebné funkce pro fungování SIP serveru. Mezi ty základní se řadí lokalizační server, registrační server, SIP proxy server, aplikační

server SIP a server pro přesměrování. K dosažení širší funkcionality využívá přídavných modulů.

Kamailio může být využito pro tvorbu velkých VoIP platforem a real-time komunikací zahrnujících WebRTC, Instant messaging apod. Také jej lze použít pro škálovatelnost SIP-PSTN brán, PBX systémů, serverů typu Asterisk, FreeSWITCH, SEMS.

1.3.4 Cisco IP comunnicator

Tento software, jak už název napovídá, pochází od firmy Cisco. Jde o softwarový telefon, který je funkcí srovnatelný s hardwarovými variantami řady Cisco 79XX. Mezi jeho výhody patří možnost využití XML aplikací, automatická detekce VPN klienta, podpora kodeků G.711 a G.729. Důležité také je, že podporuje protokol SCCP. Ten slouží ke komunikaci mezi IP telefony a Cisco Call Managerem (CCM), který lze nadefinovat v GNS3. Software je dostupný na oficiálních stránkách výrobce.

1. Uživatelské okno: ukazuje volající statusy, menu telefonu apod.
2. Kontrolní tlačítka okna: zobrazit/skrýt
3. Programovatelná tlačítka: pod tlačítko jde uložit definovanou funkci
4. Zprávy
5. Adresář
6. Tlačítko „Pomoc“
7. Nastavení
8. Servisní tlačítko
9. Nastavení hlasitosti
10. Nastavení speakeru
11. Ztišení
12. Sluchátko
13. Scroll tlačitko
14. Video
15. Klavesnice
16. Tlačítka softkey
17. Hlasová zpráva a vyzváněcí indikátor

Obrázek 1.18: Vzhled telefonu a uživatelský popis

1.3.5 X-lite

Proprietární freeware VoIP softphone vyvinut společností Counter-Path, který využívá SIP protokol. Je poskytován pro nejpoužívanější operační systémy. V roce 2005 byl v internetové telefonii zvolen jako produkt roku.

1.3.6 Yate

Jedná se o další SIP softphone. Tentokrát od firmy Yate. Software se snadno ovládá. Podporuje komunikační protokoly Jingle/Google, Talk/XMPP, H.323, IAX, SIP.

1.3.7 **Blink**

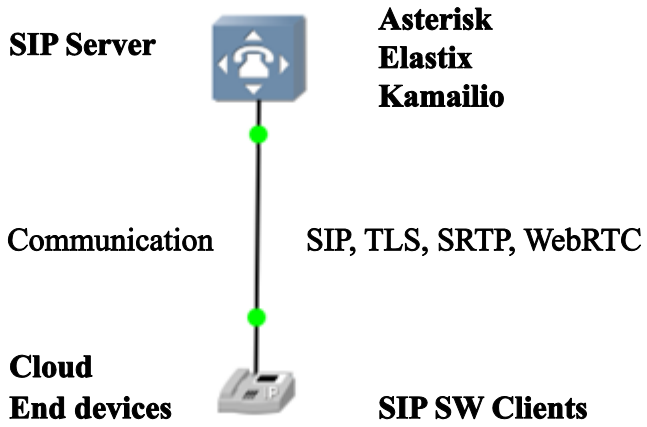
Je to softphone, jenž byl původně napsán v programovacím jazyku Python. Podporuje Windows a Linux platformy. Vhodný je především pro pokročilé uživatele. Umožňuje využití certifikačních autorit, nastavení komunikačních portů atd. Detailnější popis a jeho obsluha je demonstrována v navazujících kapitolách.

Nyní je možné říct, že byly pokryty a nastudovány všechny teoretické možnosti tvorby emulačních modelů pro IP telefonii. Zahrnujíce objasnění samotné tématiky IP telefonie a komunikačního standardu SIP, představení simulačního prostředí GNS3, uvedení využitelných emulovaných aplikací a systémů. Byly definovány pojmy, které se týkají této problematiky. Teoretický základ je tudíž popsán a nyní lze postoupit k návrhu samotných topologií neboli modelů, čímž se zabývá následující kapitola.

2 Návrh topologií IP telefonní infrastruktury

Pro výukové účely byly navrženy tři nejpoužívanější topologie s ohledem na jejich modularitu a škálovatelnost. Zároveň byl brán zřetel na maximální možnou obsazenost jednotlivých cvičení na škole, a tudíž jsou modely určeny pro počet 12 studentů.

Předpokladem pro sestavení každého modelu je nejprve vytvoření virtuálního stroje plnícího roli komplexního SIP serveru. Tato úloha je realizována pomocí softwaru VirtualBox a využití určitých popisovaných celků z podkapitoly 1.3. Zhotovený virtuální stroj je poté importován a naemulován pomocí prostředí GNS3, kde je uskutečněno jeho propojení s Cloudem. Ten představuje „univerzální“ koncové řešení topologií, pomocí něhož se mohou realizovat, připojením přes interface adresu, definované koncové uživatelské prvky. V tomto případě se bude jednat především o SIP softwarové klienty. GNS3 je zde využito hlavně z důvodu budoucí snadné rozšiřitelnosti navržených IP telefonních infrastruktur pomocí tohoto prostředí. Šablona GNS emulované topologie bude vypadat následovně:

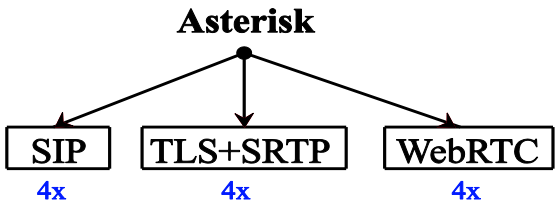


Obrázek 2.1: Šablona emulace pro GNS3

To by byla jednoduše řečeno síťová kostra, která zprostředkovává propojení mezi jednotlivými prvky infrastruktury a vytváří tím funkční komptabilitu modelu jako celku. Do této kostry je potřeba „vložit“ topologie, jež jsou dále navrženy a popsány v této kapitole. Topologie obsahují a prezentují emulované aplikace a systémy popsané v podkapitole 1.3.

2.1 Topologie č. 1

Na virtuálním stroji je nainstalován Asterisk, který v tomto případě slouží jako SIP server, ke kterému jsou připojena jednotlivá koncová zařízení v podobě softwarových klientů. Topologie využívá některých pokročilých služeb. Některé jsou typu kryptografického jako TLS a SRTP, nebo také jiného jako WebRTC. Tyto „služby“ jsou popsány níže. Při pohledu na schéma modelu lze vidět, že každá ze zmíněných částí je zprovozněna pro 4 uživatelské účty.



Obrázek 2.2: Topologie č.1

2.1.1 Transport Layer Security (TLS)

Slouží k šifrování probíhající signalizace při volání. Jedná se o praktický způsob zajišťující bezpečnost vůči nežádoucím jevům. Je tedy nemožné zjistit, která zařízení si mezi sebou volají, jaký je využívaný kodek apod. Tento chráněný druh komunikace mezi Asteriskem a SIP klientem vyžaduje vygenerování klíčů pro obě strany, modifikaci konfigurace Asterisku k zajištění podpory TLS, vytvoření SIP peer podporujícího TLS a v neposlední řadě modifikaci SIP klienta tak, aby umožňoval provozovat tuto šifrovanou komunikaci.

2.1.2 Secure Real-time Transport Protocol (SRTP)

Pro kompletní šifrování SIP komunikace je využíváno TLS a právě SRTP. Obě služby se většinou aplikují pospolu. TLS zajišťuje šifrování signalizace, ve které jsou zároveň přenášeny klíče šifrování, což je důležité hlavně pro funkčnost SRTP. To šifruje probíhající RTP pakety. Slouží jako prevence před možným odposloucháváním vedené konverzace.

2.1.3 Web Real Time Communication (WebRTC)

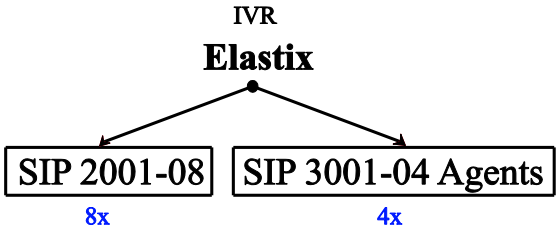
V tomto případě jde o zprostředkovávání komunikace pomocí tzv. websocketů. Jedná o poměrně novou technologii postavenou na Javascriptu a určenou k využívání prostřednictvím webových prohlížečů. Umožňuje přenos hlasu, videa, zpráv v reálném čase. Největší výhodu představuje fakt, že není potřeba instalace žádných dalších přídavných pluginů či aplikací. Vše, co uživatel v daný moment potřebuje, je webový prohlížeč a „správná“ internetová stránka. V případě této DP se bude jednat o webové stránky podporující SIPML5 klienta, který bude zaregistrován k Asterisku. Spojení je definováno jako peer-to-peer komunikace na aplikační úrovni a portu 80, tudíž nevyžaduje speciální podporu ze síťové strany.

2.2 Topologie č. 2

Je věnována komunikačnímu SIP serveru Elastix, který simuluje reálné callcentrum s většinou jeho běžných funkcí. Topologie je tvořena z osmi koncových SIP klientských účtů a čtyř dynamických agentů, kteří plní případnou roli obsluhy klientů.

V praxi to funguje tak, že klienti i agenti jsou registrováni k Elastix. Ten zaštiťuje jejich vzájemnou propojenost. Klienti si mohou volat navzájem mezi sebou nebo vytočit navolený kód pro rychlou volbu, který je odkáže do systému interaktivního průvodce. Ten je rozčleněn do několika

částí, přičemž je schopen přepojit uživatele tam, kam potřebuje, přehrát mu zadanou zprávu nebo jej zařadit do odpovídající fronty, na jejímž konci bude obsloužen agentem. Mezi další funkce patří například ukončení hovoru, automatické zopakování hlavního „menu“ atd.



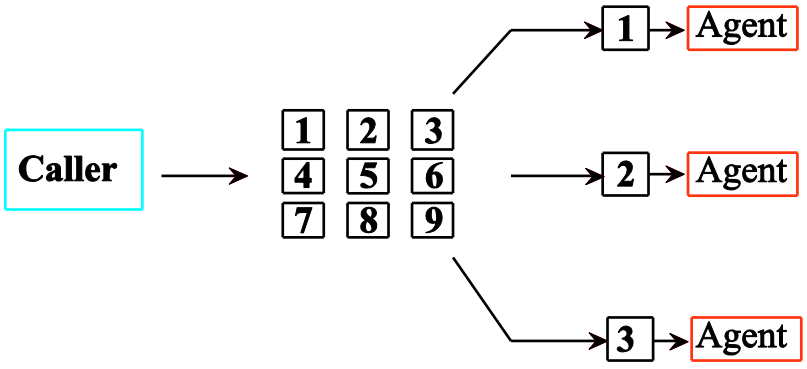
Obrázek 2.3: Topologie č.2

2.2.1 Interactive Voice Response (IVR)

Hlasový systém umožňující interakci, tzn. je schopen volajícímu přehrát, případně pomocí hlasové syntézy vygenerovat zvukové informace, na které zákazník pomocí hlasu nebo stisku DTMF kláves reaguje.

Za běžný IVR systém je často označován hlasový automat sloužící kupříkladu k výběru služby, požadovaného odborného oddělení atd. V praxi to může vypadat například tak, že se ozve hlas s větou: „K připojení do menu výběru aktivity stiskněte tlačítko 1“.

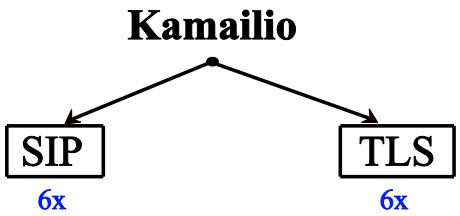
IVR systémy jsou víceúčelové a záleží především na vstupních požadavcích před samotnou realizací, jež určí, jak by měl systém pracovat, a podle toho je teprve posléze vytvořen. Je schopen řídit hovory s ohledem na denní dobu, upřednostnit zákazníka na základě rozpoznání volajícího čísla atd. V určitých případech je vhodné propojit IVR se systémem CRM, díky němuž je umožněno vést databázi o volajících. Hovory lze poté nahrávat a ukládat právě do CRM systému.



Obrázek 2.4: Příkladné schéma IVR

2.3 Topologie č. 3

Základním kamenem této poslední topologie je Kamailio, které zaštiťuje funkci SIP serveru, jelikož žádný jiný standard ani nepodporuje. Při pohledu na topologii lze vidět, že bude alokováno 6 SIP koncových klientských účtů a poté 6 účtů, které budou využívat šifrování signalizace TLS, jenž je popsáno již v topologii č.1.



Obrázek 2.5: Topologie č. 3

Cíl této kapitoly spočíval ve zužitkování nabytých teoretických informací z kapitoly č. 1 takovým způsobem, aby byly efektivně navrženy již několikrát zmiňované modely. V průběhu kapitoly jsou představeny jednotlivé modely a je popsána navržená využívaná struktura a podporované služby. Nyní lze pokročit k praktické realizaci, což je úkolem následující kapitoly.

3 Realizace a konfigurace navržených modelů

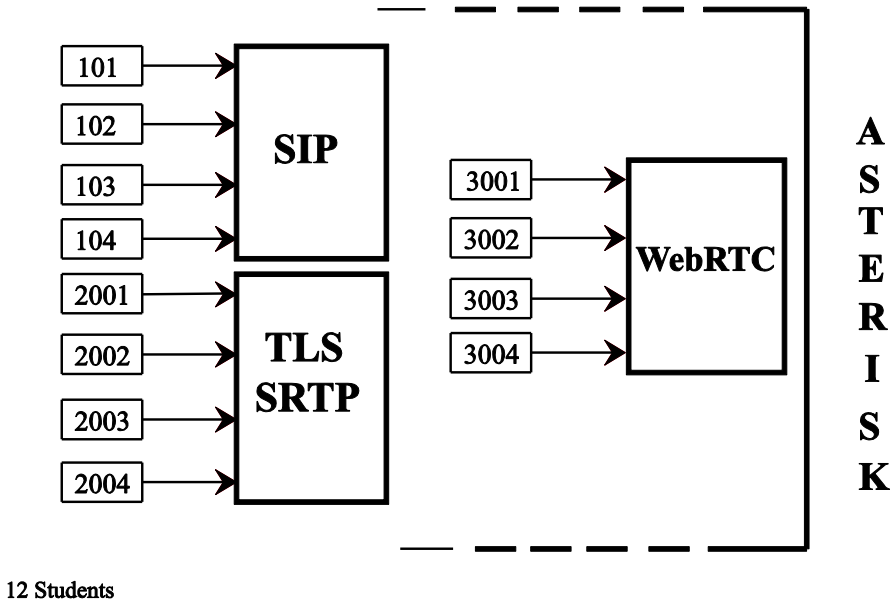
Tato část práce demonstruje krok po kroku realizaci navržených modelů z předchozí kapitoly. Je rozdělena na tři podkapitoly, z nichž se každá věnuje konkrétní topologii.

Ještě před započetím virtualizačních procesů je potřeba zkontrolovat, zda procesor konkrétního PC podporuje virtualizaci. V případě autora DP bylo potřeba vstoupit do Biosu a zvolit pokročilé nastavení, kde se musela povolit možnost virtualizace. Následoval reboot systému a poté byl již PC připraven. Výhodou pro virtualizaci je také využití 64 bitového systému.

3.1 Topologie č.1

První krok implementace představuje instalaci operačního systému, na němž bude Asterisk posléze fungovat. Z několika možností bylo vybráno Ubuntu verze 16.04, a to především z důvodu snadnější obsluhy Asterisku v tomto OS. Ubuntu je bezplatně dostupné ve 32bit a 64bit verzi s možností výběru z několika release update na oficiálních stránkách. Proběhlo tedy stažení výše zmíněné verze ISO obrazu, který bude následovně prostřednictvím VirtualBoxu spuštěn.

Nejprve došlo k vytvoření virtuálního stroje s vybraným OS, který má zajištěnou internetovou podporu prostřednictvím síťového mostu. Po spuštění Ubuntu na virtuální vrstvě je cílem otevření terminálu, kde bude probíhat postupná implementace Asterisku a služeb s ním spojených. Především pak TLS, SRTP a WebRTC. V terminálu je nutné vystupovat pod právy Roota k umožnění realizace složitějších „změn“. Přepnutí do tohoto režimu zajišťuje nainstalování root režimu a využití příkazu sudo -i. Jakmile má uživatel root práva, může prostřednictvím příkazů uvedených níže stáhnout a rozbalit instalační soubory Asterisku. Dodatečně je zde také vloženo schéma pro přehled mezi konfigurovanými účty a službami.



Obrázek 3.1: Schéma Asterisk

3.1.1 Instalace

```
wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz
tar -xvf asterisk-13-current.tar.gz
cd asterisk-13.9.1/
```

Po „přepnutí“ do složky se staženým Asteriskem je nejprve nutné provést update systému a poté již lze přejít k samotné instalaci jednotlivých částí SIP serveru.

```
apt-get update
apt-get install libc-dev libncurses-dev libssl-dev zlib1g-dev
apt-get install g++ uuid-dev libjansson-dev libxml2-dev libsqlite3-dev
apt-get install unixodbc-dev libsrtp-dev libmyodbc
./contrib/scripts/install_prereq install
./configure --with-pjproject-bundled
make -j4
make install
make config
make samples
```

Ověřit správnost instalace je možné několika způsoby. Zaprvé se uživateli zobrazí informační zpráva zahrnující Asterisk o aktuální verzi. V tomto případě jde o verzi 13.14.0. A zadruhé při pohledu do adresáře /etc/asterisk by pak měly být nalezeny jednotlivé konfigurační soubory typu sip.conf, extensions.conf apod. Samotné spuštění Asterisku se dá provést několika způsoby. Zde jsou uvedeny dva možné příkazy plnící tuto roli:

```
asterisk -r
asterisk -vvvvvvc
```

3.1.2 Konfigurace SIP účtů

Poté je možné přejít k první části konfigurace modelu, a sice nadefinovaní 4 SIP uživatelských účtů, jež budou zaregistrovány k SIP serveru a bude jim zprostředkována funkce komunikace mezi sebou. K tomuto účelu je potřeba zavítat do konfigurační složky sip.conf. Níže je přiložen screen pořízený při konfiguraci. Jsou zde nastaveny důležité parametry zahrnující přístupové heslo,

komunikační port, využité zvukové kodeky atd. Je důležité si povšimnout také položky „context“, která odkazuje do souboru extensions.conf, kde se definuje chování pro jednotlivé SIP klienty.

```
[101]
deny=0.0.0.0/0.0.0.0
type=friend
secret=1234
qualify=no
port=5060
pickupgroup=
permit=0.0.0.0/0.0.0.0
nat=no
mailbox=101@device
host=dynamic
dtmfmode=rfc2833
dial=SIP/101
context=test
canreinvite=no
callgroup=
callerid=device <101>
accountcode=
call-limit=1000
allow=ulaw
```

```
[default]
exten => _2XXX,1,Dial(SIP/${EXTEN})

[test]
exten => _1XX,1,Dial(SIP/${EXTEN})
```

Levý obrázek znázorňuje konfiguraci SIP klienta 101. Celkem jsou k dispozici 4 SIP účty v rozpětí: **101-104** s heslem: **1234**.

Obrázek nacházející se na pravé straně demonstruje možnost nastavení souboru extensions.conf. V tomto případě je nastavení založeno především pro zkompletování hovoru, což zprostředkovává aplikace „Dial“.

Obrázek 3.2, 3.3: Ukázka konfiguračních souborů sip.conf (levá strana), extensions.conf (pravá strana)

Po provedení konfigurace 4 SIP účtů je možné se postupně přesunout k nastavení SIP koncových klientů. Pro úspěšné zaregistrování jednotlivých zařízení k ústředně se musí zadat číslo neboli název vytvořeného účtu, nastavené přístupové heslo a hlavně IP adresa, na níž Asterisk běží. Pro její zjištění je třeba zadat v terminálu příkaz:

```
Ifconfig
```

V případě autora DP jde o IP adresu PC v domovské internetové síti, a sice **10.0.0.2/24**

Pokud vše odpovídá nastaveným parametrům, proběhne úspěšná registrace klientů k SIP serveru. Stav SIP zařízení lze ověřit v Asterisku pomocí příkazu:

```
Show sip peers
```

Naběhne tabulka, která indikuje stav připojených zařízení online/offline, využívaný port atd. Po těchto krocích jsou klienti úspěšně zaregistrováni k SIP serveru a je jim umožněna komunikace mezi sebou. Konkrétní otestování funkčnosti a měření dílčích parametrů bude uskutečněno v další kapitole.

Name/username	Host	Dyn	Forcerport	Comedia	ACL	Port	Status
102/102	10.0.0.1	D	No	No	A	5060	Unmonitored

Obrázek 3.4: Ukázka zaregistrovaného zařízení 102

3.1.3 Konfigurace TLS a SRTP

Další část konfigurace představuje nastavení služeb šifrovaní pro signalizaci a tok RTP paketů. Jedná se tudíž o povolení a zprovoznění služeb TLS a SRTP pro komunikaci mezi jednotlivými klienty. Uskutečnění tohoto procesu, zjednodušeně řečeno, zahrnuje vygenerování šifrovacích klíčů pro obě strany. Tyto klíče jsou poté navzájem mezi serverem a klientem vyměněny a může začít šifrovaný přenos.

První krok představuje vytvoření složky, do které budou ukládány generované klíče používané k šifrování [13].

```
mkdir /etc/asterisk/keys
```

Další v pořadí je vygenerování šifrovacích klíčů neboli certifikátů pro server. Akci je možné provést níže doplněnými příkazy. Tímto jsou klíče vytvořeny a uloženy do složky s názvem keys. Při tvorbě je důležité odkázat se na zdrojovou složku Asterisku. V tomto případě jde o cestu /usr/src/asterisk-13.14.0. Při generování je uživatel tázán na zadání sekvencí pro jednotlivé části certifikátů. Postačí zadání sekvence „1234“, ale záleží na rozhodnutí uživatele.

```
./ast_tls_cert -C pbx.mycompany.com -O "My Super Company" -d
/etc/asterisk/keys
```

- "-C" nadefinování IP adresy nebo DNS domény
- "-O" nastavení jména, typu organizace
- "-d" výstupní složka pro vygenerované klíče

Následuje vygenerování certifikátů pro klient softwarové koncové prvky. Provedení je uskutečněno pomocí příkazů níže. Jde o totožný proces s tím předešlým. Uživatel si však musí dát pozor na nastavení konkrétního SIP účtu, pro nějž je certifikát neboli klíč tvořen. Ukázková sekvence se týká například SIP účtu 2001.

```
./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k
/etc/asterisk/keys/ca.key -C 2001.mycompany.com -O "My Super
Company" -d /etc/asterisk/keys -o 2001
```

- "-m" stanovuje skutečnost, že se certifikát tvoří pro klienta
- "-c" specifikuje, který certifikát je využit
- "-k" poskytuje klíč pro certifikační autoritu
- "-C" nastaví hostname nebo IP adresu SIP klienta
- "-O" definuje jméno organizace
- "-d" výstupní složka pro vytvořené klíče
- "-o" jméno klíče, který je generován

Po uskutečnění těchto příkazů by měl obsah složky pro klíče vypadat následovně:

```
-rwxrwxrwx 1 root root 1233 bře 25 12:58 asterisk.crt
-rwxrwxrwx 1 root root  582 bře 25 12:58 asterisk.csr
-rwxrwxrwx 1 root root  887 bře 25 12:58 asterisk.key
-rwxrwxrwx 1 root root 2120 bře 25 12:58 asterisk.pem
-rwxrwxrwx 1 root root  162 bře 25 12:57 ca.cfg
-rwxrwxrwx 1 root root 1769 bře 25 12:58 ca.crt
-rwxrwxrwx 1 root root 3311 bře 25 12:58 ca.key
-rwxrwxrwx 1 root root  130 bře 25 15:52 tmp.cfg
-rwxrwxrwx 1 root root 1233 bře 25 13:01 2001.crt
-rwxrwxrwx 1 root root  586 bře 25 13:01 2001.csr
-rwxrwxrwx 1 root root  887 bře 25 13:01 2001.key
-rwxrwxrwx 1 root root 2120 bře 25 13:01 2001.pem
```

Obrázek 3.5: Vytvořené certifikační autority

Zatím se jednalo o vytvoření klíčů pro jedno koncové zařízení a server. Další problém představovala skutečnost, jak certifikáty přenést z virtuálního PC do hostitelského. K tomuto úkonu je využíván software WINSCP. Připojení k virtuálnímu serveru funguje za použití služby ssh, tedy portu 22. Před uskutečněním samotné operace je třeba nainstalovat openssh-server na virtuálním Ubuntu. Jakmile dojde k připojení výše zmíněného softwaru, mohou před samotným přenesením představovat problém ještě práva, která se ovšem dají obejít. Jednou z možností je využití příkazu na povolení všech práv pro složku s certifikáty, ze které se musí posléze přenést do hostitelského PC, kde budou vloženy do SIP softphonu. Pro tyto účely je využíván softphone s názvem Blink.

```
Chmod 777 -R /etc/asterisk/keys
```

Ovšem před tím, než se tomu tak stane, musí být jednotlivé SIP účty opět vytvořeny a „propojeny“ s vygenerovanými certifikáty. Proto je potřebné znova otevřít konfigurační adresář sip.conf, kde jsou provedeny následující změny, které ilustrují níže vložené obrázky. Lze si povšimnout, že jsou vloženy odkazy k načtení certifikátů, je povoleno šifrování atd.

```
[general]
tlsenable=yes
tlsbindaddr=0.0.0.0
tlscertfile=/etc/asterisk/keys/asterisk.pem
tlscafile=/etc/asterisk/keys/ca.crt
tlscipher=ALL
tlsclientmethod=tlsv1
tlsdontverifyserver=yes
udpbindadress=0.0.0.0
directmedia=no
qualify=yes
```

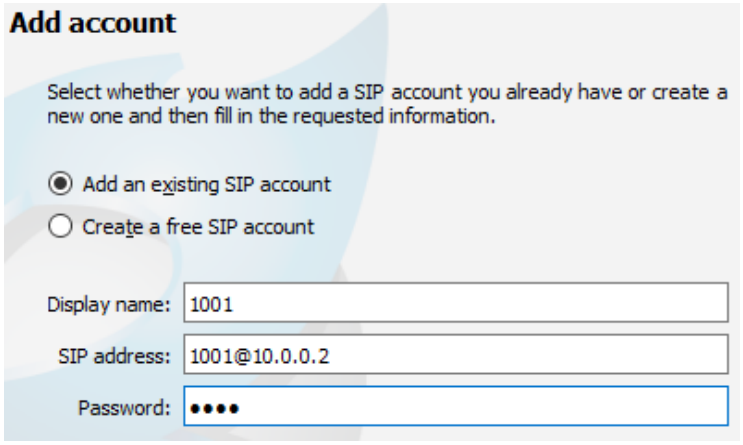
```
[2001]
type=friend
secret=1234
host=dynamic
transport=tls
encryption=yes
context=default
qualify=yes
```

Obrázek 3.6, 3.7: Klient TLS, SRTP

Jakmile je provedena registrace klienta, je téměř zajištěno, že šifrovací procesy fungují. Odzkoušení a ověření jednotlivých vlastností následuje v další kapitole.

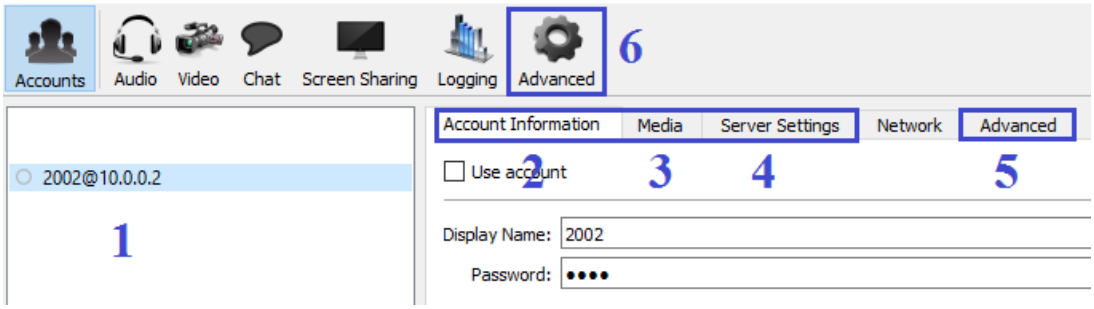
Níže je přiložen návod pro vložení certifikačních autorit, konfiguraci portů a nastavení

šifrování TLS a SRTP v softphonu Blink. Tedy kompletní registrace koncového zařízení k PBX pro zadané šifrovací služby.



Obrázek 3.8: Připojení SIP účtu

K připojení již existujícího SIP účtu, jenž byl před chvíli vytvořen, je nutné nastavit jeho parametry tak, aby bylo docíleno šifrování TLS a SRTP. Tento proces se odehrává v záložce „manage accounts“. Postup je rozdělen do několika číselných kategorií, které demonstruje následující obrázek.



Obrázek 3.9: Vytvoření SIP účtu

1) Výběr SIP účtu.

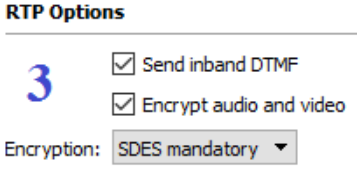
2) Jedná se o zobrazované jméno a heslo k účtu.

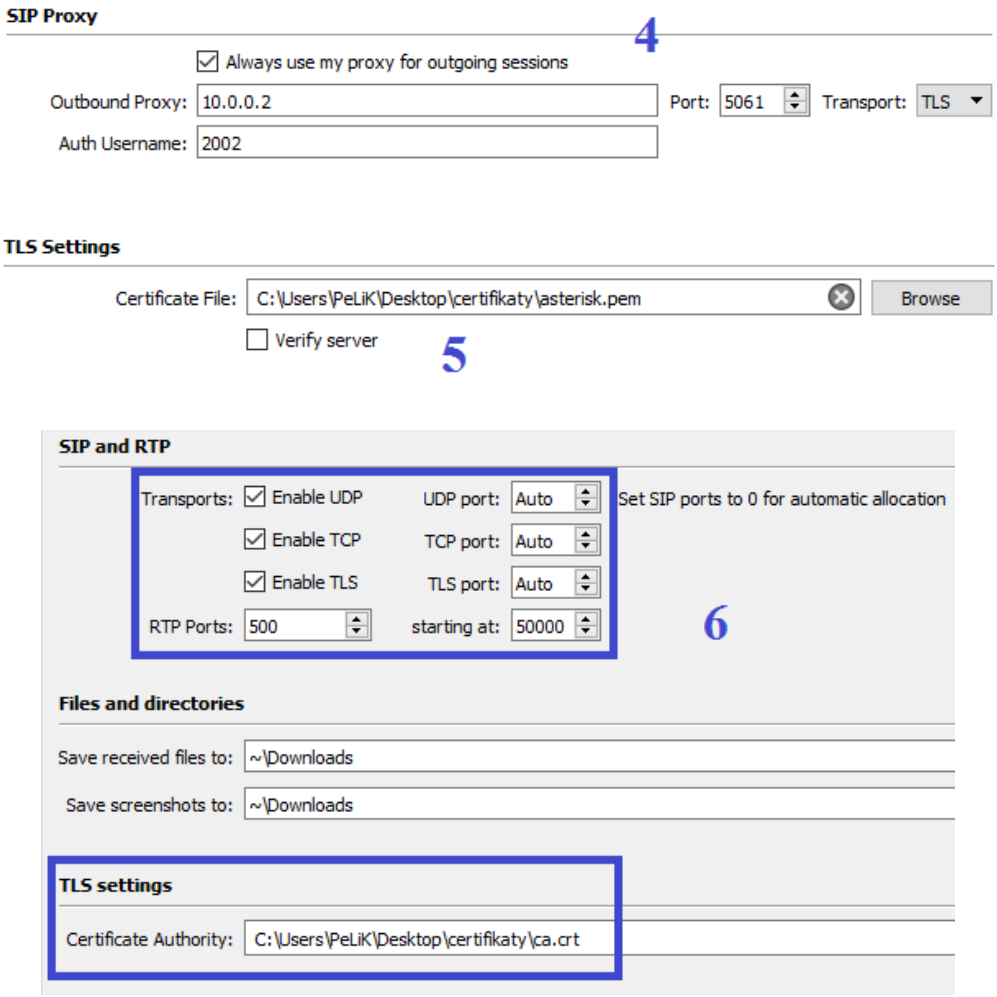
3) Nastavení šifrovaní RTP toku a výběr konkrétní šifry. V tomto případě SDES mandatory.

4) Stanovení komunikačního portu 5061 pro TLS.

5) Vložení autorizačního certifikátu pro server.

6) Pro transport je vybráno TLS a zároveň je vložen ca.crt





Pokud je dodržen následující postup, konfigurace je úspěšně nastavena a služba funguje, tak jak má. Samozřejmě softphone Blink není jediný z široké nabídky dnešních SW klientů, který v praxi umožňuje využití certifikačních autorit.

3.1.4 Konfigurace WebRTC

Stejně jako v předešlých případech je pro funkčnost této služby nutné upravit několik konfiguračních adresářů Asterisku. Uplatnit certifikační autority, které už ovšem byly vytvořeny v rámci TLS a SRTP. Musí se provést restart Asterisku a posléze se již registrovat v internetovém rozhraní k vytvořenému SIP účtu pomocí světově prvního open source HTML5 SIP klienta. K nalezení je na webových stránkách společnosti Doubango. Komunikace probíhá pomocí websocketů. Nicméně zpět na začátek. První krok představuje editace adresáře http.conf, ve kterém je nutné zajistit konfiguraci webového serveru. Náhled konfigurace se nachází níže.

```
[general]
enabled=yes;
bindaddr=10.0.0.2;
bindport=8088;
tlsenable=yes;
tlsbindaddr=10.0.0.2:8089
tlscertfile=/etc/asterisk/keys/asterisk.pem
tlsprivatekey=/etc/asterisk/keys/asterisk.pem
```

```
[general]
rtpstart=10000
rtpend=20000
icesupport=yes
stunaddr=stun.l.google.com:19302
```

Obrázek 3.10, 3.11: Ukázka http.conf (vlevo) a rtp.conf (vpravo)

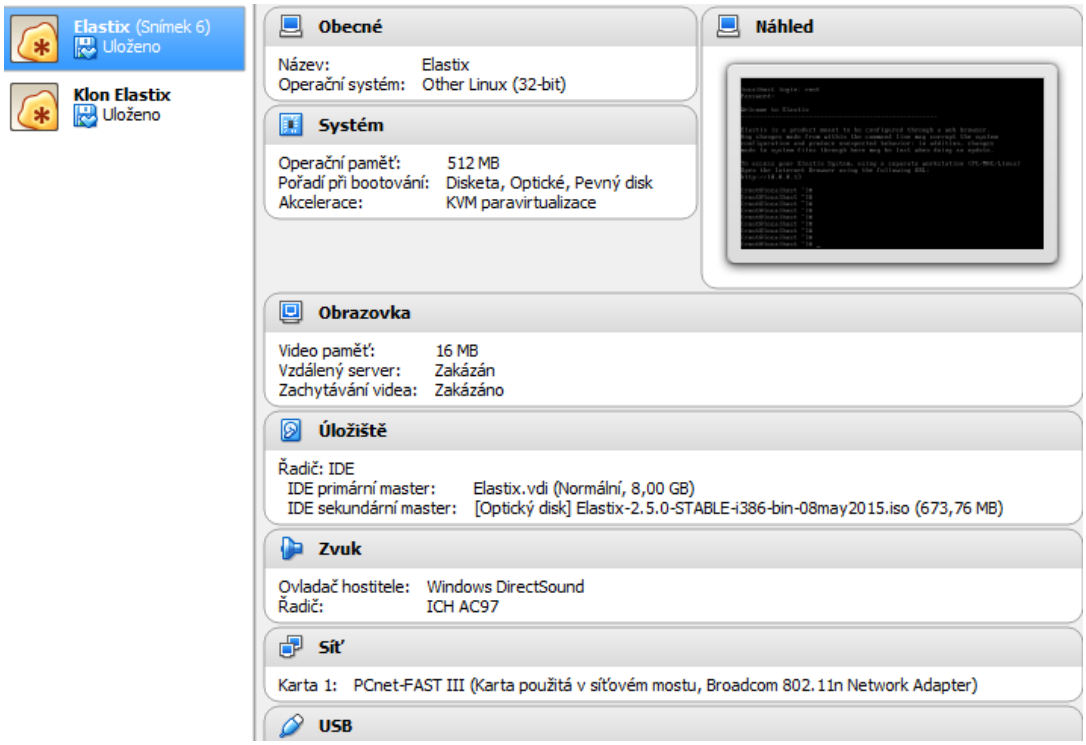
Sekunduje editace adresáře sip.conf, což je nastavení koncových uživatelských účtů pro podporu této služby. Příklad nakonfigurovaného účtu se nachází níže. Jednou z věcí, která je ještě doporučována je zkontrolování firewall brány, zda propouští potřebné porty. Poté stačí jen restartovat asterisk a registrovat se pomocí SIP HTML5 klienta k serveru. Ukázka tohoto procesu je v následující kapitole.

```
[3001]
type=friend
username=3001 ; The Auth user for SIP.js
host=dynamic ; Allows any host to register
secret=1234 ; The SIP Password for SIP.js
encryption=yes ; Tell Asterisk to use encryption for this peer
avpf=yes ; Tell Asterisk to use AVPF for this peer
icesupport=yes ; Tell Asterisk to use ICE for this peer
context=default ; Tell Asterisk which context to use when this peer is dialing
directmedia=no ; Asterisk will relay media for this peer
transport=udp,ws,wss ; Asterisk will allow this peer to register on UDP or WebSockets
dtlsenable=yes ; Tell Asterisk to enable DTLS for this peer
dtlsverify=no ; Tell Asterisk to not verify your DTLS certs
dtlscertfile=/etc/asterisk/keys/asterisk.pem ; Tell Asterisk where your DTLS cert file is
dtlsprivatekey=/etc/asterisk/keys/asterisk.pem ; Tell Asterisk where your DTLS private key is
dtlssetup=actpass
force_avp=yes
```

Obrázek 3.12: Ukázka sip.conf

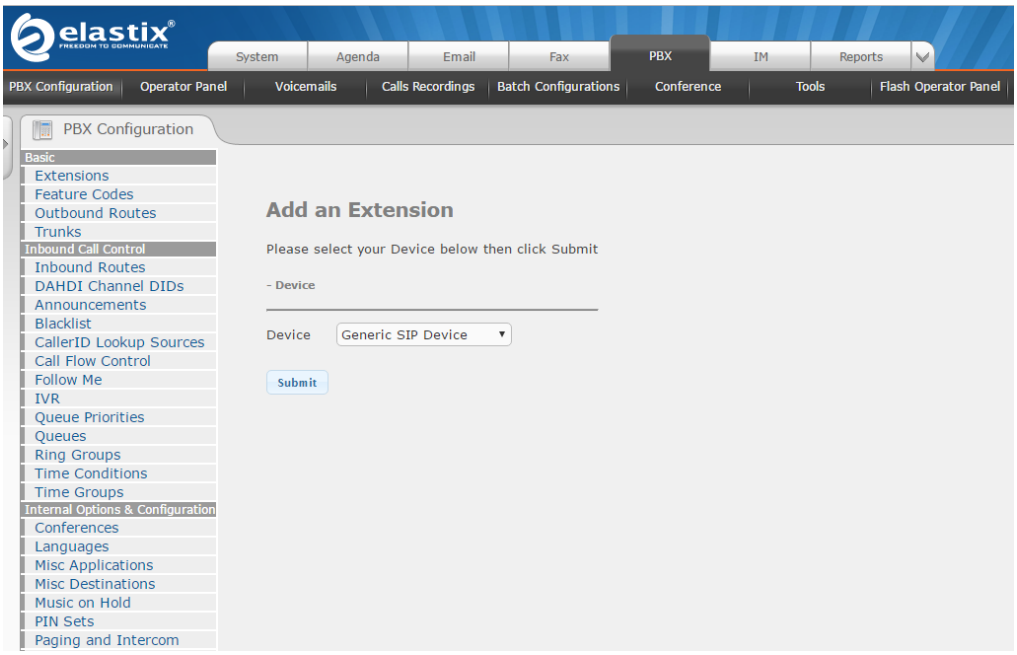
3.2 Topologie č. 2

Nejprve je potřeba realizovat Elastix SIP server. Nejsnazší cestou je zavítání na oficiální webové stránky distributora, kde je možno si vybrat z aktuálně nabízených verzí. Jedná se o verze 5.0 a 2.5, přičemž byla z důvodů autorova méně výkonného PC vybrána verze 2.5. Proběhlo stažení ISO obrazu, který byl posléze naimportován do virtuálního softwaru Virtualbox. Vytvořený virtuální stroj disponuje operačním systémem „Other“ Linux 32bit a parametry vybranými tak, aby byla jeho realizace a provoz na hostitelském stroji bezproblémový. Důležité je také nastavení sítě, je nutné zajistit internetovou dostupnost pro „virtuál“. Z toho důvodu byla vybrána možnost síťového mostu, který zprostředkovává spojení s reálnou sítí pomocí vygenerované síťové karty. Náhled nastavených parametrů viz následující obrázek.



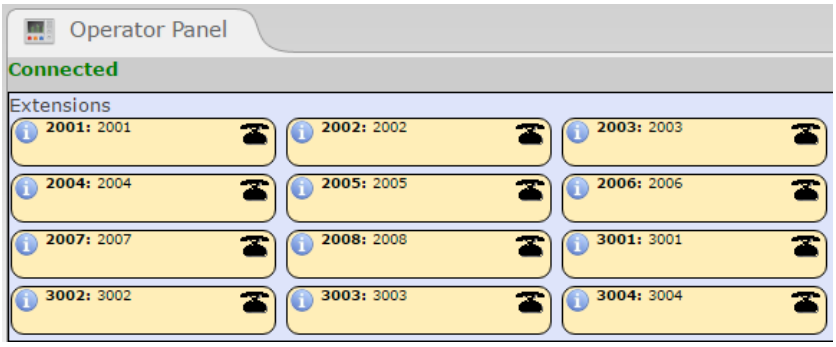
Obrázek 3.13: Virtuální stroj Elastix

Samotná instalace Elastix zahrnuje vybrání časového pásma, nastavení uživatelských hesel pro jednotlivé části a také přidělení IP adresy pro SIP server. Byla zvolena možnost DHCP, tudíž její automatické přidělení. Po dokončení instalace je nutné přihlásit se jako „root“ a zadat nastavené uživatelské heslo. Spustí se okno Elastix, kde oznamuje vygenerovanou IP adresu pro server. Při zadání této IP adresy do internetového prohlížeče lze vstoupit do konfiguračního GUI. Je potřeba přihlásit se jako admin a opět zadat nastavené heslo. Konfigurační GUI obsahuje informační panel PBX a všechny potřebné záložky k vytvoření kompletního callcentra. V tomto případě byl Elastix server tvořen v domácí síti a běží na adrese 10.0.0.13. Uživatelské GUI Elastix zobrazuje obrázek 3.14.



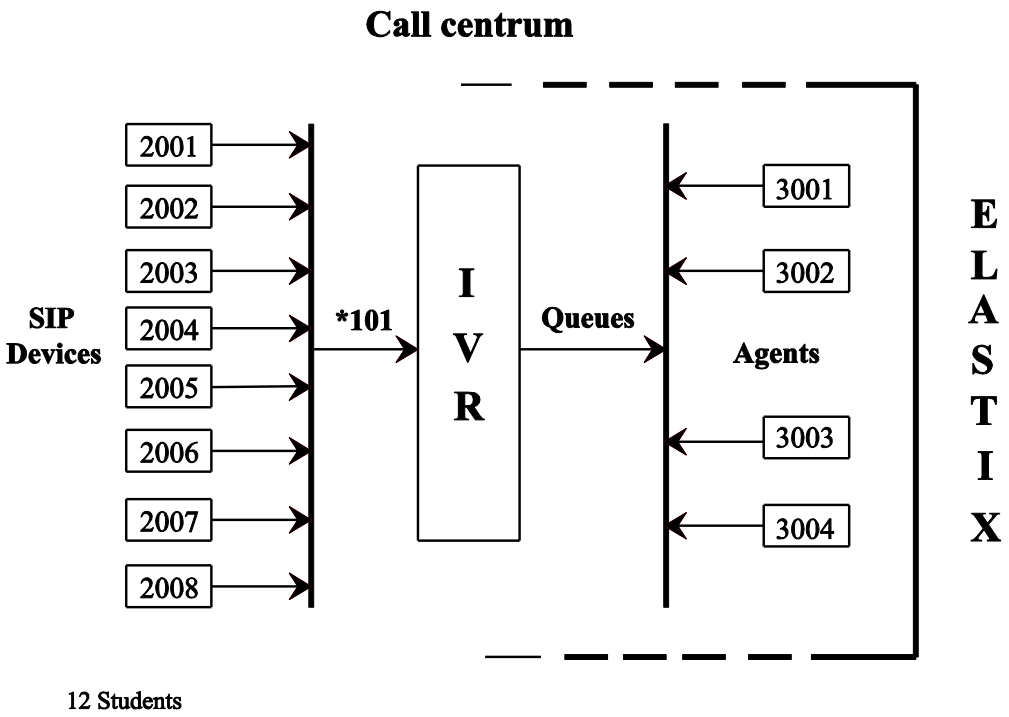
Obrázek 3.14: Konfigurační GUI Elastix

Při tvorbě callcentra je využíváno záložek zobrazených na levé části obrázku. Prvním krokem je vytvoření koncových SIP uživatelů přes záložku „Extensions“. Důležité je vyplnit položky: User Extension, SIP Alias a Secret, která nastaví heslo pro připojení SIP klienta k PBX. Po dokončení tohoto kroku vypadá seznam koncových zařízení následovně: 2001-2008 SIP devices, 3001-3004 Agents.



Obrázek 3.15: Nadefinovaná koncová zařízení

Nyní je nutné vytvořit zvukovou databázi potřebnou pro obsluhu jednotlivých operací, které bude callcentrum poskytovat. Zvukové stopy se nahrávají v záložce „System Recordings“. Než se ovšem podniknou další fáze konfigurace, je potřeba uvést koncept konkrétního callcentra, jež je implementováno.

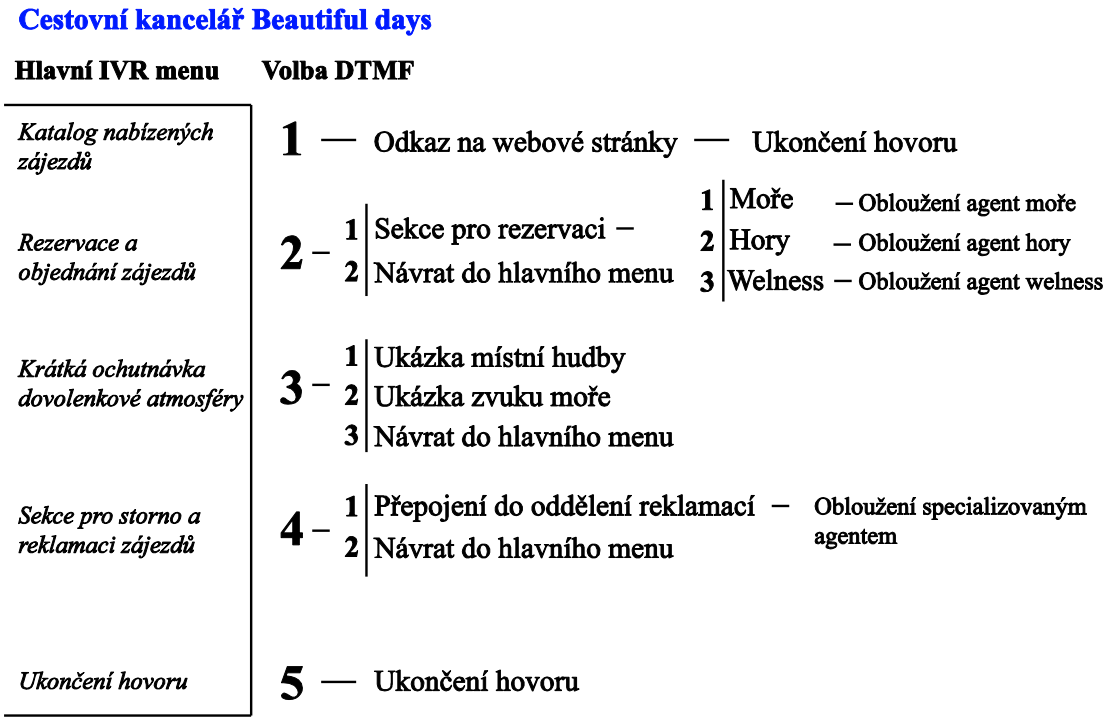


Obrázek 3.16: Schéma Elastix callcentra

Při pohledu na schéma callcentra je možné vidět, jak je navrženo a jak funguje. SIP klienti si mohou volat mezi sebou. Při vytočení kódu *101 jsou odkázáni na IVR, kde jsou pomocí nahraných a nadefinovaných hlasových relací navedeni k „cíli“. To znamená, že jsou například přepojeni do specializovaného oddělení, kde budou obslouženi agentem nebo je jim přehrána odpovídající hlasová zpráva, jsou odkázáni na webové stránky, jiného odborníka apod. Pokud je aktuální agent momentálně zaneprázdněn, jsou uživatelé zařazováni do odpovídajících front. Toť ve zkratce ke schématu Callcentra. Konkrétnímu nastavení jednotlivých částí callcentra a jejich detailnějšímu popisu je věnována pozornost při postupné konfiguraci.

Jakmile je zhotovena zvuková databáze, je možno pokročit k vytvoření úvodního menu, které uživateli zazní při vstupu do IVR. Nejprve je potřeba zvolit záložku „IVR“, kde je zmíněná vstupní část nadefinována. Poté je v záložce „Misc Applications“ nastaveno, že pro vstup do tohoto IVR musí volající zadat *101. Vstupní menu se sestává z pěti kategorií simulujících kompletní chod vymyšlené cestovní kanceláře. Každé odvětví je „schováno“ pod určitou DTMF volbou.

Při vstupu do menu je volajícímu přehrána welcome zpráva, která má za úkol provést jej schématem callcentra. Snaží se ho navést do konkrétní sekce, kde bude obsloužen. Účastník se pohybuje po menu IVR stiskem DTMF kláves. Koncept je navržen takovým způsobem, aby se volající mohl ve většině případů vrátit do úvodního menu. Jedná se v podstatě o cyklus, ze kterého je možné vystoupit pouze pomocí stisku tlačítka 5. Výjimku zde tvoří pouze menu 1, které po přehrání zadané stopy ukončí hovor samovolně. IVR schéma vymyšlené cestovní kanceláře a jeho logistické uspořádaní se nachází na obrázku 3.17.



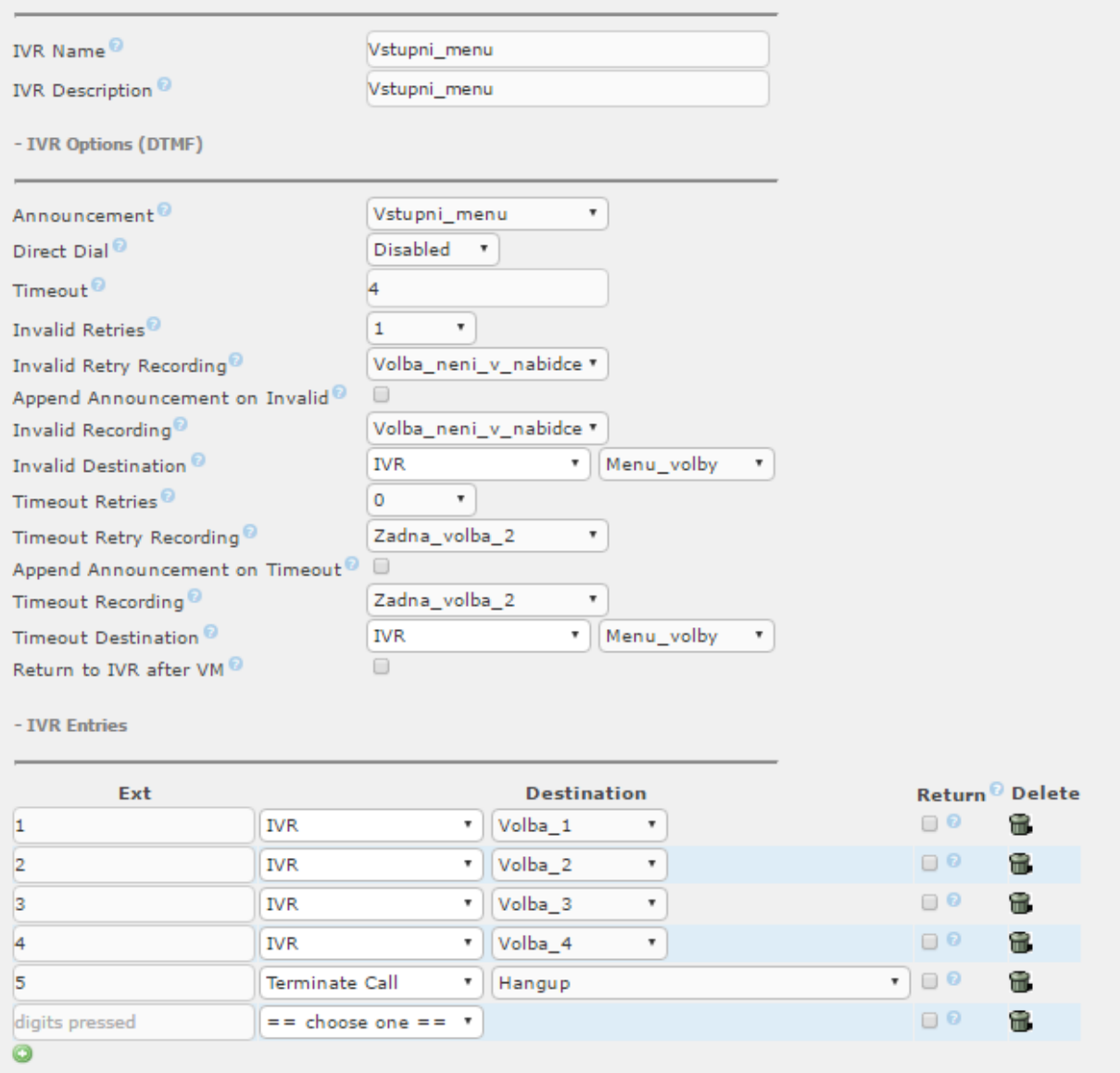
Obrázek 3.17: Schéma IVR

Při pohledu na schéma je možné v jeho levé části vidět konkrétní procesy, uložené pod jednotlivými DTMF volbami. Některé se dále dělí pomocí využití dalších IVR menu, některé přecházejí k přepojení volajícího na agenta, zabývajícího se konkrétní problematikou. Jsou i takové, které přehrají nahranou zprávu nebo ukončí hovor.

3.2.1 Tvorba a funkce IVR

Tato podkapitola objasňuje tvorbu a funkce spojené s IVR. Taktéž bude popsáno sestavení vstupního menu pro call centrum cestovní kanceláře „Beautiful days“. Byly nastaveny tyto parametry:

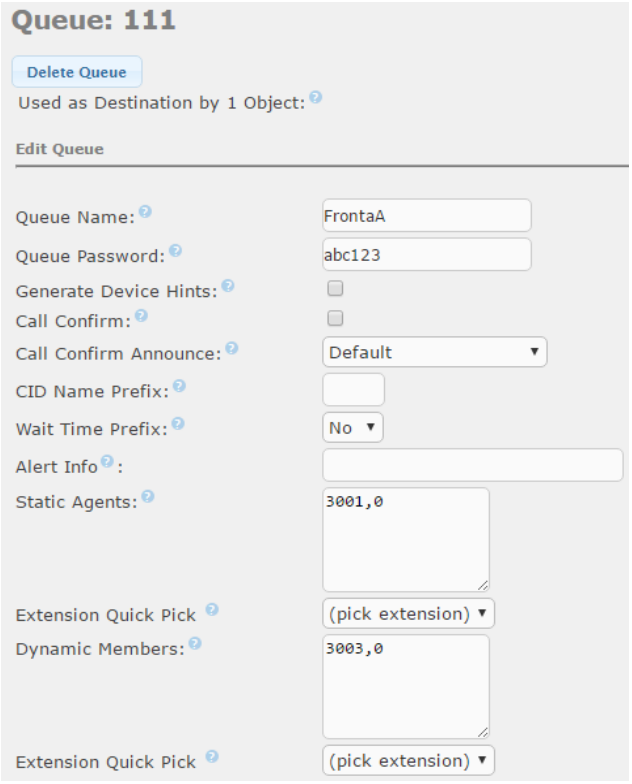
- **Announcement:** Přehraje zadanou zvukovou stopu při vstupu do IVR „Vstupní menu“.
- **Invalid Recording:** Při zadání nenadefinované DTMF volby přehraje zvukovou stopu označující chybnou volbu.
- **Invalid Destination:** Cíl, kam je volající nasměrován po zadání „špatné“ volby. V tomto případě je naveden do vytvořeného záložního menu pro volbu.
- **Timeout Recording:** Přehraje se, pokud není po dobu nastaveného timeoutu zaznamenána jakákoliv DTMF volba ze strany volajícího.
- **Timeout Destination:** Cíl, kam je volající přesměrován při nezadání žádné volby.
- **IVR Entries:** Definuje operace, jež se odehrají při stisku vybrané klávesy. V případě čísel 1-4 se jedná o přechod do dalších IVR, utvořených pro jednotlivé sekce. Stisk 5 pak znamená ukončení hovoru. Kromě těchto dvou zmíněných funkcí je možnost vybrat si ze široké škály dalších definovaných procesů, ať už řazení do front, zanechání hlasové zprávy, přesměrování na konkrétní koncové zařízení atd. To záleží však na uživateli, jak si Elastix PBX nadefinuje. Zde se nachází screen z nadefinovaného hlavního menu:



Obrázek 3.18: Vytvořené hlavní menu IVR

V tomto bodě je zhotovena konfigurace SIP klientů a agentů, potřebné IVR a jednotlivé sekce pro výběr, nahrány všechny potřebné zvukové tóny, je nakonfigurována vstupní kódová sekvence, jsou doladěny jednotlivé situace, kdy například účastník „zmáčkne“ špatnou volbu, nebo naopak po určitou dobu není aktivní. Nyní je zapotřebí zajistit situace, při kterých dochází k přepojení volajícího na konkrétního člověka neboli agenta plnícího roli obsluhy. Jinak řečeno, musí se vytvořit fronty zahrnující pravidla pro řazení, nadefinovat lidi sedící na jejich konci apod.

Zmíněná operace se provádí v záložce „Queues“. Tam je možno vytvořit frontu s „lidmi“, kteří ji budou obsluhovat, nastavit strategii při vyčkávání, maximální počet čekajících lidí ve frontě a spoustu dalších věcí. Ukázka zhotovené fronty se nachází na další stránce.



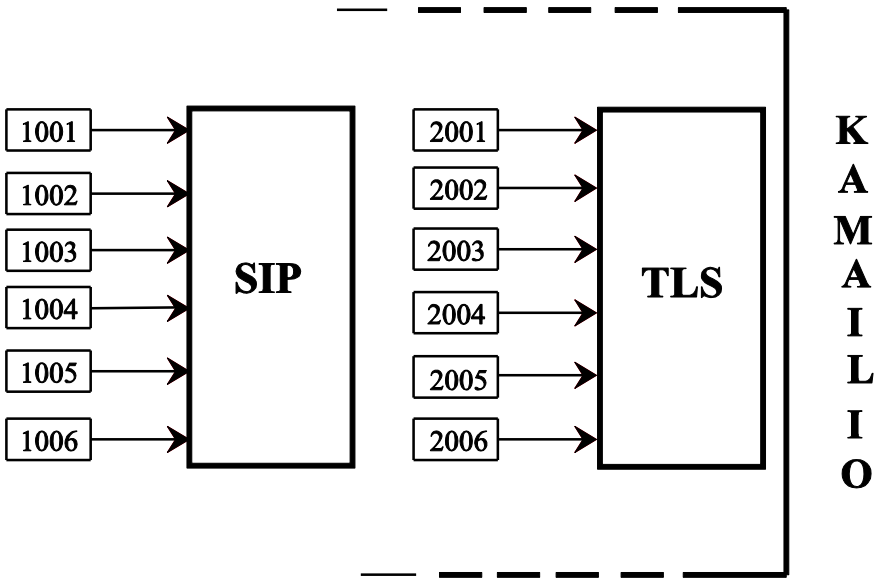
Jedná se o frontu s názvem FrontaA a číslem 111. Pro přístup a administraci je nastaveno heslo „abc123“. Přiřazení konkrétních agentů k frontám je provedeno v položce „Static Agents“. Pokud se scrolluje níže, je možno nalézt konkrétní nastavení toho, jak se fronta má chovat. Co se týče front v tomto modelu, jsou vytvořeny tři konkrétní, přičemž 2 slouží k objednání různých dovolenkových destinací a jedna k reklamaci (agent hory a wellness je jeden). Jedná se konkrétně o DTMF volby 3 a 4. Tam jsou zmiňované fronty aplikovány.

Obrázek 3.19: Vytvoření fronty

Elastix běží již při startu virtuálního počítače s potřebným ISO obrazem a může aktivně sloužit jako PBX. Po provedení konfigurace je již možné připojit koncová zařízení pomocí zadání čísla SIP účtu, hesla potřebného k ověření a IP adresy, na níž nainstalovaný SIP server běží. Tato varianta připojení koncových prvků byla úspěšně odzkoušena a provedena na základě otestovaní správného nastavení Elastix dle kritérií, které byly navrženy.

3.3 Topologie č.3

Tento model se skládá především ze SIP proxy serveru Kamailio. Zde je přiloženo opět schéma pro přehled:



Obrázek 3.20: Schéma Kamailio

Je nezbytné nejdříve provést aktualizaci všech dostupných balíčků, jež podporují jeho komplexní funkčnost [14].

```
apt-get install update
apt-get install upgrade
```

Po proběhnutí aktualizace nezbytných částí je možno přejít ke stažení a nainstalování potřebných modulů.

```
apt-get install mysql-server
apt-get install kamailio kamailio-tls-modules
mysqlserver // vytvoření databáze a zvolení hesla
cd /etc/kamailio
nano /etc/kamailio/kamctlrc
```

Nyní je potřeba provést editaci výše otevřeného souboru. Tento proces demonstruje následující obrázek, v němž jsou zobrazeny jen ty nejdůležitější řádky konfigurace, vybrané z celého adresáře.

```
SIP_DOMAIN=10.0.0.2
DBENGINE=MYSQL
DBHOST=localhost
DBNAME=kamailio
DBRWUSER="kamailio"
DBRWPW="kamailiorw"
DBROUSER=kamailioro
DBROPW=kamailioro
DBROOTUSER="root"
VERBOSE=1
PID_FILE=/var/run/kamailio/kamailio.pid
```

Obrázek 3.21: Ukázka konfigurace adresáře kamctlrc

```
kamctl add 1001 1234 // vytvoření SIP účtu 1001 s heslem 1234
kamctl rm // slouží k odstranění existujícího SIP účtu
kamctl ul show // výpis připojených klientů
kamctl db show subscriber // výpis obsahu databáze
```

Výše popsanými příkazy lze docílit vytvoření jednotlivých SIP účtů a také jejich registraci k SIP serveru. V tento moment již fungují a jsou schopny navázat mezi sebou spojení. Jedná se o účty v rozpětí: **1001-1006** přístupné pod heslem: **1234**.

Další krok představuje konfigurace SIP účtů, jejichž signalizace je šifrována pomocí TLS. Jedná se o účty v rozmezí: **2001-2006** s heslem: **1234**. K tomu je potřeba ověření oboustranného spojení pomocí certifikátů. Zde jsou využity certifikáty, které již byly vytvořeny v rámci konfigurace prvního modelu. K tomuto účelu slouží také vytvořená složka etc/kamailio/keys, kde jsou naimportovány tyto zmiňované klíče. Jedná se hlavně o asterisk.pem a asterisk.key. Rovněž je zapotřebí pro plnou funkčnost TLS nainstalovat ca certifikát na hostitelském PC. Po provedení instalace je nutné editovat adresář kamailio.cfg, kde se musí povolit modely pro podporu TLS, MYSQL, AUTH a nastavit port naslouchající TLS službě. Editaci demonstruje obrázek 3.22.

```
nano kamailio.cfg
```

```
#!define WITH_MYSQL
#!define WITH_AUTH
#!define WITH_TLS
```

```
#listen=tls:10.0.0.2:5061
```

Obrázek 3.22: Ukázka konfigurace adresáře kamailio.cfg

Jeden z posledních kroků inicializace Kamailio představuje editace adresáře tls.cfg, jenž nastavuje prepozice pro TLS. Opět jsou vloženy certifikáty, stanovena metoda šifrování atd.

```
nano tls.cfg
```

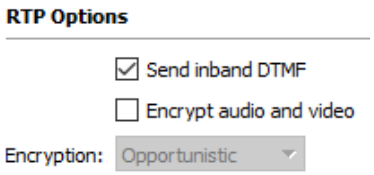
```
[server:default]
method = TLSv1
verify_certificate = yes
require_certificate = no
private_key = /etc/kamailio/keys/asterisk.key
certificate = /etc/kamailio/keys/asterisk.pem
#ca_list = ./modules/tls/cacert.pem
#crl = ./modules/tls/crl.pem
[client:default]
verify_certificate = no
require_certificate = no
[server:10.0.0.2:5061]
method = SSLv23
verify_certificate = no
require_certificate = no
private_key = /etc/kamailio/keys/asterisk.key
certificate = /etc/kamailio/keys/asterisk.pem
#verify_depth = 3
#ca_list = local_ca.pem
#crl = local_crl.pem
```

Obrázek 3.23: Ukázka konfigurace adresáře tls.cfg

Následuje ujištění se faktu, že po správné konfiguraci se Kamailio spustí. V návaznosti na to je proveden restart služby. Poté je možné již SIP proxy aktivně využívat.

```
nano /etc/default/kamailio
RUN_KAMAILIO = yes
service kamailio restart
```

Připojení SIP klientských zařízení již bylo popsáno a realizováno v rámci topologie č.1. Jediná změna se udává při TLS. Pokud chce uživatel registrovat SIP účet s podporou TLS musí „vypnout“ šifrování RTP toku. Jedná se opět o softwarovém klientu Blink, stejně jako v případě topologie Asterisk.



Obrázek 3.24: Vypnutí šifrování RTP

4 Testování funkčnosti a měření dílčích IP telefonních parametrů vytvořených modelů

Tato kapitola se zabývá demonstrováním funkčnosti a měřením jednotlivých parametrů vztažených k vytvořeným modelům z předešlé kapitoly.

4.1 Topologie č.1

Nejprve musí být otestována schopnost vytvořených SIP účtů registrovat se k Asterisku. Tudíž jsou z repertoáru nakonfigurovaných účtů vybrány tyto dva následující: 101 a 102, které se připojí k SIP serveru a poté mezi sebou uskuteční hovor. Funkci softwarových klientů v tomto případě realizují Yate a X-Lite. Po spuštění Asterisku lze zahájit proces registrace. Jsou spuštěni zmínění SIP klienti a proběhlo zadání čísla účtu, adresy serveru a přístupového hesla. Následně se v Asterisku zobrazí zpráva, která informuje uživatele o tom, že při naslouchání na UDP portu 5060 server zaznamenal požadavek pro registraci koncového zařízení. Pokud souhlasí všechny nastavené údaje, proběhne registrace. Tuto akci demonstruje navazující obrázek, kde je možno vidět zmiňovanou informační zprávu.

```
*CLI>       -- Registered SIP '102' at 10.0.0.1:56515
         > Saved useragent "X-Lite release 4.9.8 stamp 84253" for peer 102
```

Obrázek 4.1: Registrace účtu 102 (X-Lite) k Asterisku

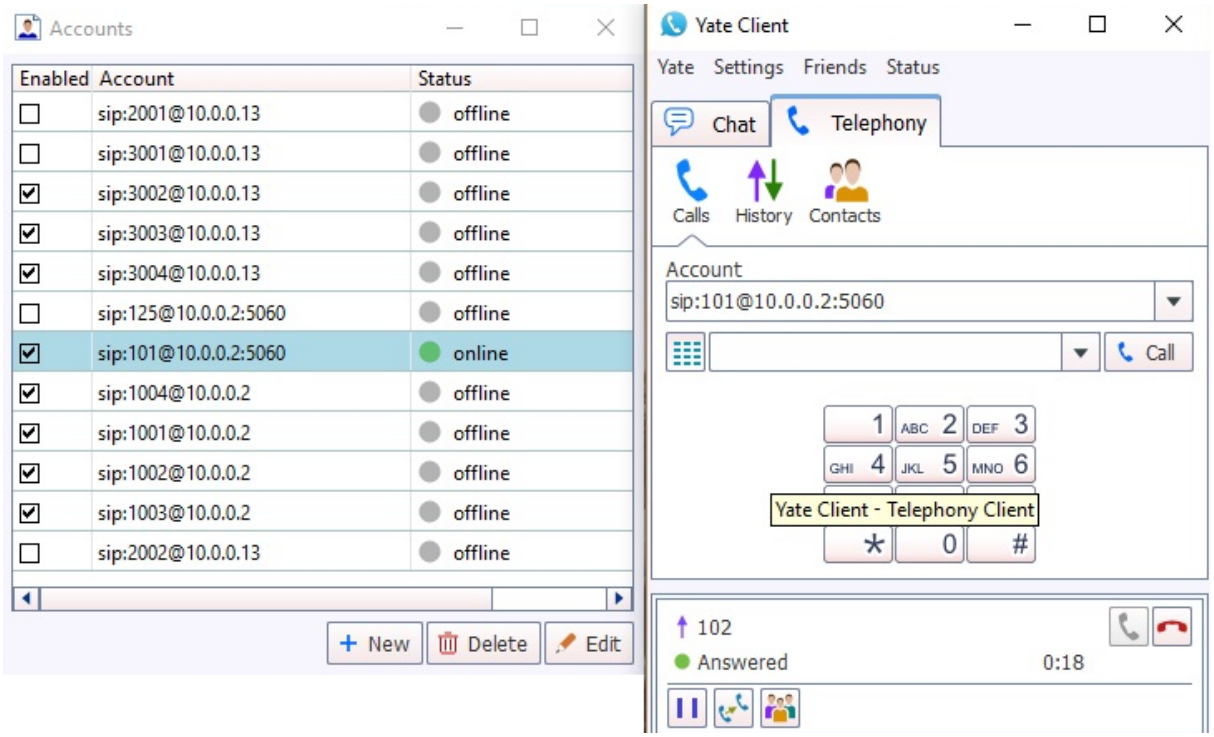
Poté je využita aplikace Dial, tedy je uskutečněn testovací hovor z jednoho klienta na druhého. V tomto případě bude klient 101 (Yate) volat na klienta 102 (Xlite). Při vytočení čísla 102 je uskutečněno vyzvánění a po přijetí hovoru druhou stranou je možné vyzkoušet, zda probíhá korektně i RTP komunikace. Spojení bylo tedy úspěšně navázáno a proběhla i výměna RTP paketů, kterou je možné posléze analyzovat ve Wiresharku.

Kdyby byl náhodou klient 102 už zaneprázdněn, ozve se obsazovací tón. Zde je možné vidět na obrázku uskutečnění hovoru z pohledu informačních zpráv v Asterisku. Ty obsahují souhrnná data o hovoru, využité procesy atd.

```
== Using SIP RTP CoS mark 5
  -- Executing [102@test:1] Dial("SIP/101-00000004", "SIP/102") in new stack
== Using SIP RTP CoS mark 5
  -- Called SIP/102
  -- SIP/102-00000005 is ringing
     > 0x7f85ac008990 -- Probation passed - setting RTP source address to 10.0.0.1:54972
  -- SIP/102-00000005 answered SIP/101-00000004
  -- Channel SIP/102-00000005 joined 'simple_bridge' basic-bridge <dce47a8a-a7c7-4402-92bc-c3d31a5fe862>
  -- Channel SIP/101-00000004 joined 'simple_bridge' basic-bridge <dce47a8a-a7c7-4402-92bc-c3d31a5fe862>
     > Bridge dce47a8a-a7c7-4402-92bc-c3d31a5fe862: switching from simple_bridge technology to native_rtp
     > Locally RTP bridged 'SIP/101-00000004' and 'SIP/102-00000005' in stack
     > Locally RTP bridged 'SIP/101-00000004' and 'SIP/102-00000005' in stack
     > 0x7f8608006590 -- Probation passed - setting RTP source address to 10.0.0.3:20704
     > 0x7f85ac008990 -- Probation passed - setting RTP source address to 10.0.0.1:54972
  -- Channel SIP/102-00000005 left 'native_rtp' basic-bridge <dce47a8a-a7c7-4402-92bc-c3d31a5fe862>
  -- Channel SIP/101-00000004 left 'native_rtp' basic-bridge <dce47a8a-a7c7-4402-92bc-c3d31a5fe862>
== Spawn extension (test, 102, 1) exited non-zero on 'SIP/101-00000004'
```

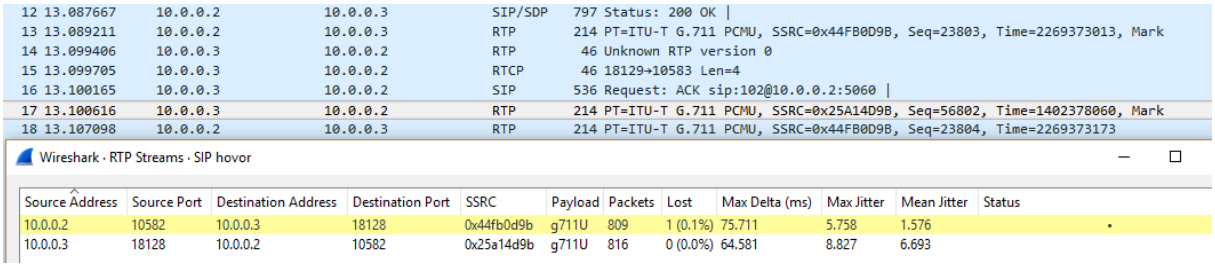
Obrázek 4.2: Výpis uskutečněného hovoru Asterisk

Při uskutečnění výše zmíněného hovoru klientem Yate byl pořízen přiložený snímek, kde je možné vidět zaregistrovaný účet 101 a jeho probíhající hovor s klientem 102.



Obrázek 4.3: Uskutečnění hovoru z pohledu SIP softwaru Yate

Tento hovor byl rovněž zachycen pomocí softwaru Wireshark a nyní zde bude podroben analýze. Wireshark umožnuje zobrazení proběhlé signalizace, schéma sestavení hovoru a také je možné vidět proběhlou RTP komunikaci. Jednotlivé parametry zachyceného hovoru jsou dostupné níže.

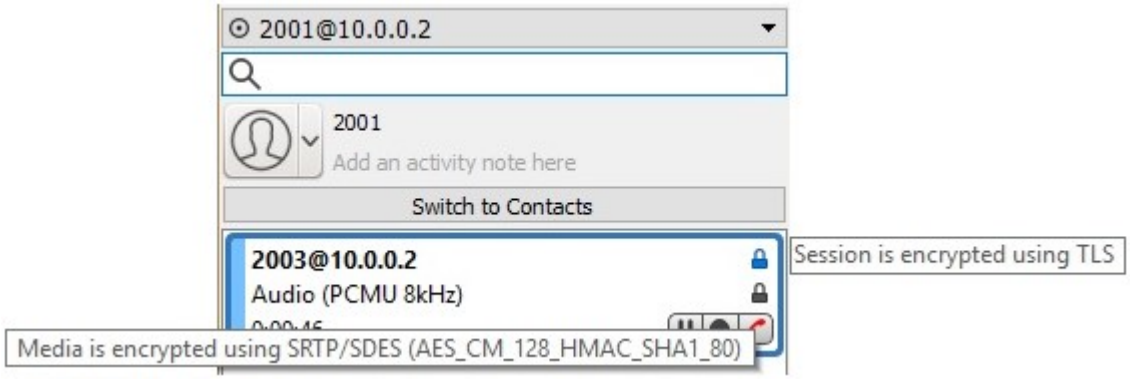


Obrázek 4.4: Výpis Wireshark

Tímto lze říct, že 4 dostupné SIP účty jsou úspěšně otestovány a vše funguje tak, jak má. Nyní je možno přejít k předvedení šifrování pomocí TLS a SRTP. Asterisk je v tomto případě nastaven tak, aby naslouchal na portu 5061. A pokud nesouhlasí certifikáty mezi serverem a koncovým zařízením, dojde k neúspěšnému pokusu o registraci. Pokud se tedy klient dokáže přihlásit k SIP serveru, svědčí to o korektním vytvoření certifikačních autorit a správném nastavení konfiguračních souborů

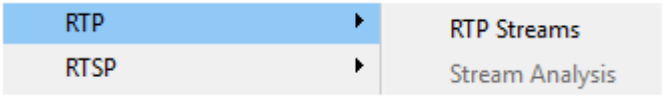
zahrnujících funkci TLS a SRTP. K předvedení odpovídající funkčnosti je využíván softwarový klient Blink, který je popsán detailněji v kapitole č. 3. Byly podniknuty konfigurační kroky zmíněné v předešlé kapitole a nyní je realizován hovor mezi klienty 2001 a 2003. V tomto případě klient 2001 (Blink) běží na PC č.1 (IP 10.0.0.2) a klient 2003 (Blink) běží na PC č. 2 (IP 10.0.0.3). Hovor byl opět odchycen pomocí Wiresharku a nyní je podroben analýze.

Již při navázání hovoru je v softphonu Blink vidět, že šifrování funguje, což dokazuje i následující obrázek:



Obrázek 4.4: Výpis uskutečněného hovoru Asterisku

Modrá ikona zámku značí využití šifrování pomocí TLS a černý zámek reprezentuje šifrování pomocí SRTP. Nicméně se jedná v podstatě jen o určité ikony v programu. Na otázku, zda to opravdu vše funguje tak, jak má, odpoví analýza odchyceného toku. Ten se nachází pod tímto textem. Při zobrazení RTP streamu se tentokrát vygeneruje prázdné okno. Pokud jde o analýzu je možné vidět, že nejde ani v záložce otevřít.



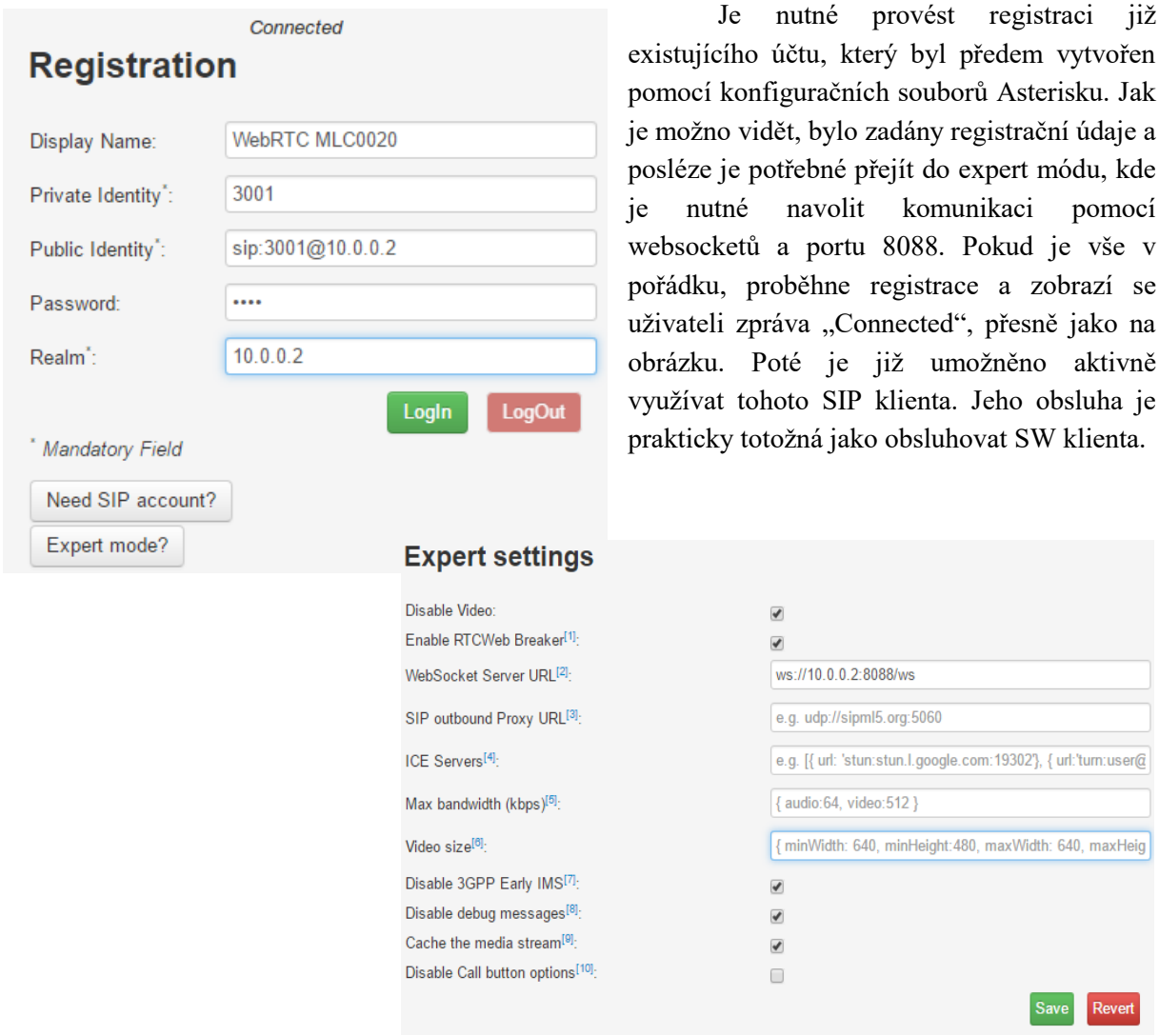
Obrázek 4.5: RTP Stream

14	10.298048	10.0.0.3	10.0.0.2	UDP	44 5060→5060 Len=2
15	11.922674	10.0.0.3	10.0.0.2	TLSv1.2	1151 Application Data
16	11.925140	10.0.0.2	10.0.0.3	TCP	60 5061→52282 [ACK] Seq=609 Ack=1922 Win=1452 Len=0
17	11.926348	10.0.0.2	10.0.0.3	TLSv1.2	648 Application Data
18	11.926916	10.0.0.3	10.0.0.2	TLSv1.2	454 Application Data
19	11.976222	10.0.0.2	10.0.0.3	TCP	60 5061→52282 [ACK] Seq=1203 Ack=2322 Win=1452 Len=0
20	11.976347	10.0.0.3	10.0.0.2	TLSv1.2	1311 Application Data
21	11.978166	10.0.0.2	10.0.0.3	TCP	60 5061→52282 [ACK] Seq=1203 Ack=3579 Win=1452 Len=0
22	11.984723	10.0.0.2	10.0.0.3	TLSv1.2	600 Application Data
23	12.035228	10.0.0.3	10.0.0.2	TCP	54 52282→5061 [ACK] Seq=3579 Ack=1749 Win=254 Len=0
24	12.116527	10.0.0.2	10.0.0.3	TLSv1.2	616 Application Data
25	12.174029	10.0.0.3	10.0.0.2	TCP	54 52282→5061 [ACK] Seq=3579 Ack=2311 Win=252 Len=0
26	15.527863	HonHaiPr_0d:c3:1b	Broadcast	ARP	42 Who has 10.0.0.138? Tell 10.0.0.3
27	15.530668	ZyxelCom_0b:78:30	HonHaiPr_0d:c3:1b	ARP	42 10.0.0.138 is at 5c:f4:ab:0b:78:30
28	19.862420	10.0.0.2	10.0.0.3	TLSv1.2	981 Application Data
29	19.865761	10.0.0.3	10.0.0.2	TLSv1.2	473 Application Data
30	19.872584	10.0.0.2	10.0.0.3	UDP	224 15556→50012 Len=182
31	19.875767	10.0.0.3	10.0.0.2	UDP	120 50013→15557 Len=78
32	19.875973	10.0.0.3	10.0.0.2	UDP	64 50012→15556 Len=22
33	19.876085	10.0.0.3	10.0.0.2	UDP	120 50013→15557 Len=78
34	19.891753	10.0.0.3	10.0.0.2	UDP	64 50012→15556 Len=22

Obrázek 4.6: Zachycený hovor při použití TLS a SRTP

Již pohled na zachycená data obrázku 4.6 navozuje fakt, že RTP stream není veřejný oproti předešlému analyzovanému hovoru. Rovněž nelze zobrazit proběhlou signalizaci, a tudíž není možné ani zjistit, mezi kterými klienty bylo spojení navázáno. Dá se tedy říct, že účty předpřipravené pro TLS a SRTP náležitě fungují.

Poslední část konfigurace modelu Asterisku představují klientské účty podporující technologii WebRTC. V tomto případě je nutné zavítat na stránky společnosti Doubango, kde je bezplatně dostupný HTML5 SIP klient, pomocí něhož je možné přihlásit se k vytvořeným účtům v rozmezí 3001-3004. Asterisk v tomto případě naslouchá na portu 8088. Při přihlašování je důležité využít staršího internetového prohlížeče, především Mozilly Firefox. Jelikož například Google Chrome blokuje vytvoření komunikace pomocí websocketů z důvodu možných bezpečnostních rizik. Proces přihlášení SIP klienta k serveru vykresluje obrázek 4.7. Po přihlášení samozřejmě následuje testovací hovor.



Je nutné provést registraci již existujícího účtu, který byl předem vytvořen pomocí konfiguračních souborů Asterisku. Jak je možno vidět, bylo zadány registrační údaje a posléze je potřebné přejít do expert módu, kde je nutné navolit komunikaci pomocí websocketů a portu 8088. Pokud je vše v pořádku, proběhne registrace a zobrazí se uživateli zpráva „Connected“, přesně jako na obrázku. Poté je již umožněno aktivně využívat tohoto SIP klienta. Jeho obsluha je prakticky totožná jako obsluhovat SW klienta.

Obrázek 4.7: Registrace WebRTC klienta

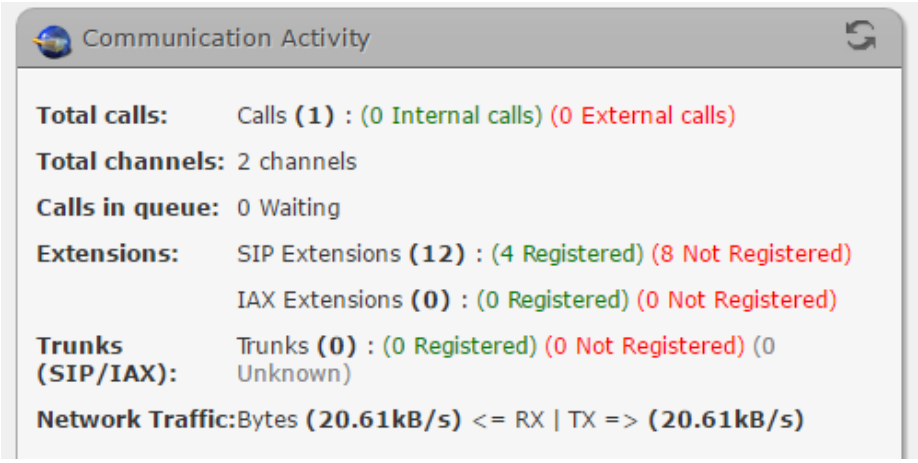
4.2 Topologie č.2

Zahrnuje otestování vytvořeného Callcentra běžícího na platformě Elastix. V tomto případě funguje Elastix na IP adrese 10.0.0.13, přičemž je při jejím zadání do webového prohlížeče dostupné konfigurační rozhraní. Popsané části je možné si prohlédnout na těchto obrázcích:

Obrázek 4.8: Vstup do konfiguračního rozhraní a info o IP adrese serveru

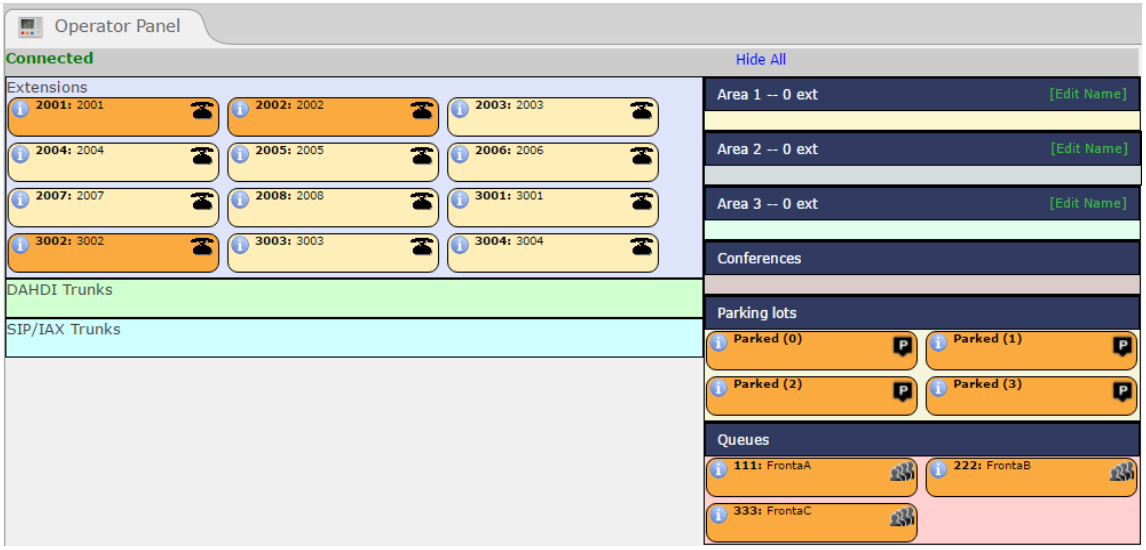
Za jednu z mnoha výhod tohoto SIP serveru lze považovat graficky výborně zpracovaný kontrolní panel plnící informační roli. Rovněž je toto prostředí více uživatelsky přátelské pro začínající uživatele. Nicméně zpět k informačnímu panelu, jenž zde bude využit k ukázce úspěšného přihlášení klientů k Elastix a poté k dalším případným úkonům.

V tomto případě slouží k předvedení funkčnosti, kdy příkladem jsou zaregistrováni 4 SIP klienti. Přitom je nutné pamatovat, že Elastix, jako jediný z těchto tří zmiňovaných SIP serverů, vyžaduje heslo složené v kombinaci z písmen a čísel. Zde je využito hesla: abc123. Při pořízení screenu zrovna probíhá hovor mezi dvěma účastníky. Informační panel je dostupný zde:



Obrázek 4.9: Informační panel (Dashboard) Elastix

Zaregistrování jednotlivých účastníků a také spojení mezi nimi tudíž funguje. Kromě všeobecného panelu přímo vztaženého k základním informacím Elastixu, který zde již byl zobrazen, existuje také kontrolní panel pro PBX určený přímo pro přehled mezi připojenými zařízeními. Jedná se o „operator panel“. V tomto případě je možné vidět, zaregistrovaná zařízení (tmavé pole), vytvořené fronty atd.



Obrázek 4.10: Operator Panel Elastix

Call centrum je ovšem založeno především na principu IVR. To využívá nahraných zvukových stop, které jsou spouštěny podle nastaveného schématu. Zde funguje podle vymyšleného schématu fingované cestovní kanceláře „Beatiful days“. Ten byl vložen již v předchozí kapitole.

4.3 Topologie č.3

Kamailio zde platí za jednu z nejjednodušších možností realizace SIP proxy serveru. Instalace je velice intuitivní a jednoduchá. I samotný proces vytvoření SQL databáze není složitý. Pokud je správně vytvořena, při inicializaci SIP účtů dochází k jejich uložení právě do této databáze. Obsah SQL je vypsán a demonstrován na tomto obrázku:

```
root@Pelik-VirtualBox:/etc/kamailio# kamctl db show subscriber
database engine 'MYSQL' loaded
Control engine 'FIFO' loaded
mysql: [Warning] Using a password on the command line interface can be insecure.
+----+----------+----------+----------+---------------+----------------------------------+----------------------------------+------+
| id | username | domain   | password | email_address | ha1                              | ha1b                             | rpid |
+----+----------+----------+----------+---------------+----------------------------------+----------------------------------+------+
|  4 | 1001     | 10.0.0.2 | 1234     |               | 731f936aae574c36aa201ca5e3ecac2f | d841b303ea6e02bb0c5276f4e08a7530 | NULL |
|  5 | 1002     | 10.0.0.2 | 1234     |               | 4ef439b8f7faaee9f6b6cc83f9161142 | b1f611a3bab0bf183af18093ec9aae3d | NULL |
|  6 | 1003     | 10.0.0.2 | 1234     |               | 2ef4120485e2dd880b99e9c6b69af0d0 | 0e7394a09df38d53add04ccf77f1977a | NULL |
|  7 | 1004     | 10.0.0.2 | 1234     |               | b4c9a3ebbb3579eba56a782607a2cd83 | e9c419548f8a395503f3595b59ed49c6 | NULL |
|  8 | 1005     | 10.0.0.2 | 1234     |               | de23e44949fa04234c9cb88334c3b4d6 | 0a14d4f3ff9b9dff0b779c0555de33df | NULL |
|  9 | 1006     | 10.0.0.2 | 1234     |               | 297f24b6de93f496ce14ec43d9b4b580 | c102e51b657298532c2e14f1adb1cb71 | NULL |
| 10 | 1007     | 10.0.0.2 | 1234     |               | cef91e28a45d2493bec46633ee0c066a | 0d0eb98ad24db9f9c3404817e6af1764 | NULL |
| 11 | 1008     | 10.0.0.2 | 1234     |               | 78725ad82257106affbe54ec8f87585d | 6ddfb988a4959e03f83bd776f4262417 | NULL |
| 12 | 2001     | 10.0.0.2 | 1234     |               | 99e257f62330501fb9c1f2e0cc1ce395 | 35420dc74bd90d2c16d3779a31cdf5b8 | NULL |
| 13 | 2002     | 10.0.0.2 | 1234     |               | ff6caa5ae3e3d333db5683e8ffc12948 | 71c39f2efa4635bcd093954fbbcb8819 | NULL |
| 14 | 2003     | 10.0.0.2 | 1234     |               | 762b3157c1fa6ff4f333ed757f8dfa24 | 3c3bb267a8c150ce0b2ecf020cb703d9 | NULL |
| 15 | 2004     | 10.0.0.2 | 1234     |               | 047e311a8dea32cb4576d00dcd167126 | fa528b0f4093616a6e29bb1dffb92465 | NULL |
| 16 | 2005     | 10.0.0.2 | 1234     |               | 79810b00a48a22cd3b05218dd3ab2246 | de9e35ca6e30a615eb9cc318f9346d38 | NULL |
| 17 | 2006     | 10.0.0.2 | 1234     |               | 5fa95aa9869a4be1a78d503e7d55de5b | b1a62bfa9880c38f10c4734947abfa3f | NULL |
| 18 | 2007     | 10.0.0.2 | 1234     |               | 6a6021b786ec2cdb7e876e2de4a83645 | 385f85c7ae797f7674fc576f29bcff15 | NULL |
| 19 | 2008     | 10.0.0.2 | 1234     |               | 6d175775321005ccda35e2f1ee428d17 | 943797f9bb6023f2cc7ec9418ad3cec0 | NULL |
+----+----------+----------+----------+---------------+----------------------------------+----------------------------------+------+
```

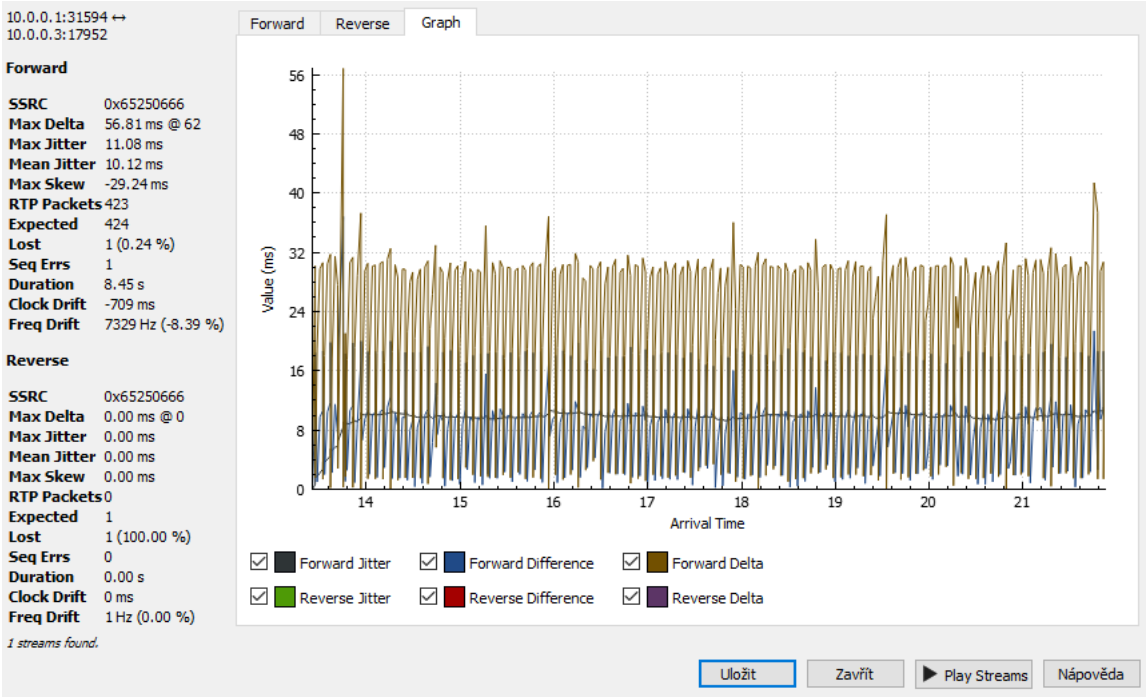
Obrázek 4.11: Výpis MySQL Kamailio

Ukázka registrovaného klienta využívaného ke službě TLS se nachází pod touto kapitolou. Jedná se o účet 2001.

```
root@Pelik-VirtualBox:/etc/kamailio# kamctl ul show
database engine 'MYSQL' loaded
Control engine 'FIFO' loaded
entering fifo_cmd ul_dump
Domain:: location table=1024 records=1 max_slot=1
        AOR:: 2001
                Contact:: sip:87530429@10.0.0.1:5061;transport=tls Q=
                        Expires:: 219
                        Callid:: ef945b85a8944deb89a143324e93cf7c
                        Cseq:: 2
                        User-agent:: Blink 3.0.0 (Windows)
                        State:: CS_NEW
                        Flags:: 0
                        Cflag:: 0
                        Socket:: tls:10.0.0.2:5061
                        Methods:: 4294967295
                        Ruid:: uloc-58da496f-4f42-1
                        Instance:: <urn:uuid:f2fd9c31-d3dc-423f-ab7f-051d6537f53a>
                        Reg-Id:: 0
                        Last-Keepalive:: 1490700873
                        Last-Modified:: 1490700873
FIFO command was:
:ul_dump:kamailio_receiver_20349
```

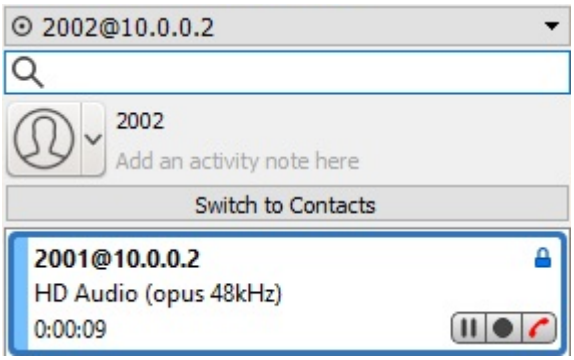
Obrázek 4.12: Ukázka registrovaného klienta 2001

Stejně jako v případě Asterisku, i zde jsou podniknuty testovací hovory za účelem ověření funkčnosti SIP a TLS. Zachycená data jsou viditelná v navazujících obrázcích, na kterých jsou na rozdíl od předchozích hovorů podrobena jiným dostupným analýzám. Obrázek 4.13 informuje uživatele o dosažených parametrech běžného hovoru. Rovněž je možné si pomocí tlačítka „Play Streams“ přehrát uskutečněný hovor.



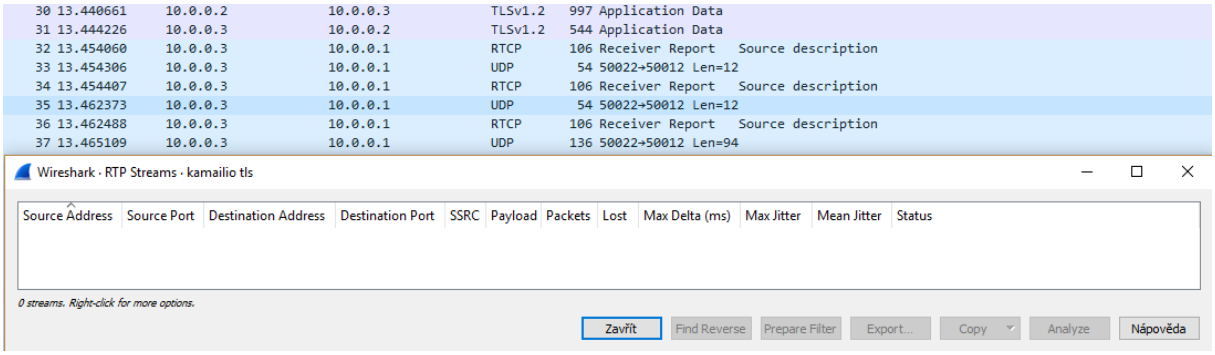
Obrázek 4.13: Technické parametry proběhlého hovoru

Posledním krokem je prezentace uskutečněného hovoru za využití TLS, jelikož Kamailio zatím nepodporuje funkci SRTP. Tento fakt je možné vypozorovat i ze zachyceného hovoru, a to skrze svítící ikoně modrého známku značící využití TLS.



Obrázek 4.14: Kamailio TLS

Sekunduje zachycený stream. Je důležité si povšimnout skutečnosti, že není možné zobrazit zařízení, mezi kterými byl hovor uskutečněn, tudíž TLS funguje správně.



Obrázek 4.15: Zachycený hovor TLS

Všechny navržené služby byly nakonec úspěšně realizovány a odzkoušeny. Jediný problém představovalo WebRTC, které je občas „náladové“ a funguje jen v určitém webovém prohlížeči. Modely jsou tedy kompletně funkční a schází vypracování uživatelské dokumentace, kterou demonstruje následující kapitola.

5 Uživatelská dokumentace

Tato kapitola se zabývá tvorbou uživatelské dokumentace, jež zahrnuje informace a zkušenosti, získané vypracováním této práce. Dokumentace je určena ke studijním účelům, především studentům na cvičeních z předmětů, orientovaných na tématiku IP telefonie. Konkrétně se jedná o školní předměty VoIP, Spojovací soustavy, Bezpečnost v komunikacích a Multimediální komunikace. Obsah dokumentace je orientován k obsluze a praktickému otestování vytvořených modelů. Ty jsou předpřipraveny pro 12 studentů s možností snadné rozšiřitelnosti dle aktuální potřeby.

Hlavní účel spočívá především v umožnění jednodušší a pokročilejší konfigurace ústřednových prvků, kdy základní nastavení je již součástí uvedených šablon. Ke každé topologii je tedy vytvořena uživatelská dokumentace v podobě pdf souboru, který je vložen do přílohy této práce.

V praxi to bude vypadat tak, že studenti zavítají na jedno ze cvičení zmíněných předmětů, kde obdrží zhotovený model a návod k jeho obsluze. Následně budou provádět úkony nadefinované v rámci této dokumentace, kdy nejprve model spustí v simulačním prostředí GNS3. Posléze dojde k naběhnutí virtuálních strojů, kde zadají přihlašovací údaje a v terminálu si spustí daný SIP server, jež je již nakonfigurován. Po těchto krocích zbývá jen vybrání konkrétního učtu zastupujícího danou službu. Jakmile se studenti rozdělí do skupin a obdrží konkrétní účet mohou provést jeho registraci prostřednictvím SIP klienta, k již spuštěnému SIP serveru.

Po uskutečnění výše popsaných kroků se mohou přesunout k praktické práci s modelem, kde otestují dílčí nadefinované služby a porozumí dané problematice. Tj. v rámci prvního modelu si vyzkouší práci s Asterisk, kdy otestují navázání klasické SIP komunikace, možnosti šifrování, komunikaci pomocí websocketů. Díky druhému modelu v podobě Elastix se seznámí se smyšleným schématem cestovní kanceláře, jež simuluje funkčnost reálného call centra. A třetí model v podobě Kamailio je obeznámí v podstatě s jednodušší a lépe dostupnou verzí Asterisku, jež zvládá klasickou SIP komunikaci, TLS šifrování a další možnosti, které se mohou případně doplnit.

Závěr

Hlavním cílem této diplomové práce bylo vytvoření komplexního výukového materiálu pro účely porozumění moderním telefonním telekomunikačním způsobům založeným na softwarové bázi. Jedná se tedy o vypracování teorie a poté vytvoření uživatelských modelů, které budou sloužit studentům k praktické výuce dané problematiky.

Nejprve bylo zapotřebí nastudovat celistvou problematiku IP telefonie zahrnující SIP protokol a poté také možnosti emulace díky virtualizačnímu prostředí GNS3. Tyto nabyté zkušenosti byly uplatněny při návrhu tří emulovaných telefonních modelů, každý je tvořen soudobými prvky IP telefonie využívanými denně ve spoustě celosvětových společností. Každý model podporuje jiný typ SIP serveru počínaje Asteriskem, jeho grafickou a uživatelsky více přívětivou variantou v podobě Elastix, a v poslední řadě pak určitým způsobem odlehčenou verzí SIP proxy v podobě Kamailio. V návaznosti na návrh jednotlivých modelů sekunduje jejich kompletní popis zahrnující podporované služby a jelikož jsou navrženy pro využití na školních cvičeních, byly koncipovány pro 12 studentů, což je běžný maximální počet obsazenosti. Samozřejmě jdou modifikovat i pro větší počet.

Jakmile došlo ke zhotovení teoretické části, bylo nutné přejít k její praktické realizaci. Při postupné komplementaci byly zaevidovány všechny důležité kroky tak, aby měl zaujatý čtenář této práce plnohodnotný návod k případné volnočasové realizaci jednotlivých topologií. Důležitou součástí procesu návrhu každého nového prvku je v praxi otestování jeho funkčnosti a dílčích parametrů, což zprostředkovává kapitola 4. Zároveň proběhlo zformování konkrétní osnovy utvářející náplň jednoho, možná dvou školních cvičení, kdy studenti budou obeznámeni jednak s teoretickou, tak i praktickou stránkou věci. Budou se řídit dle vytvořených pokynů, a přitom využívat předpřipravených modelů, jejichž komplementace byla cílem této práce.

Zmiňované modely se podařilo vytvořit a odzkoušet tak, aby fungovaly všechny navrhnuté služby. Zároveň bylo při realizaci využito virtuálního prostředí GNS3, tudíž topologie mohou být v budoucnu využity jako určitý základ a nadále se rozšiřovat dle uvážení a potřeby.

Co se týče celkového zhodnocení práce, mohu říct, že zmíněná problematika byla velice atraktivní ke studiu a realizaci. Musel jsem se sice potýkat s úskalími v podobě špatně dostupných materiálů k implementaci a v určitých případech úplné absence návodů k realizaci dílčích služeb SIP serverů. Každopádně jsem si při vypracování této práce osvojil nové zkušenosti s VoIP, na které budu moci snad v budoucnu navázat.

Použitá literatura

[1] SETHI, Adarshpal S. a Vasil Y. HNATYSHIN. The practical OPNET user guide for computer network simulation. Boca Raton, FL: CRC Press, c2013. ISBN 9781439812051.

[2] ABOELELA, Emad. Network simulation experiments manual. 5th ed. Oxford: Elsevier Science [distributor], c2011.

[3] HLAVENKA, Jiří. Výkladový slovník výpočetní techniky a komunikací: 5500 pojmů z oblasti výpočetní techniky: přes 7000 křížových vazeb: výklad anglických a českých odborných pojmů. 3. vyd. Praha: Computer Press, 1997. ISBN 80-7226-023-5.

[4] VOZŇÁK, Miroslav. Voice over IP. Ostrava: VŠB-Technická univerzita Ostrava, 2008. ISBN 978-80-248-1828-3.

[5] KELLY, Timothy. VoIP for dummies. Indianapolis, Ind.: Wiley Pub., c2005. ISBN 0764588435.

[6] WALLACE, Kevin. VoIP bez předchozích znalostí. Brno: Computer Press, 2007. Cisco systems. ISBN 978-80-251-1458-2.

[7] BAZALA, David. Telekomunikace & VoIP telefonie I. Praha: BEN-Technická literatura, 2006. ISBN 80-7300-201-9.

[8] NEUMANN, Jason C. The book of GNS3: build virtual network labs using Cisco, Juniper, and more. ISBN 1593275544.

[9] WELSH, Chris. GNS3 Network Simulation Guide, 2013.

[10] GOLDEN, Bernard. Virtualization for dummies (R). Indianapolis: Wiley Publishing, c2008. Bestselling computer book series, 1. ISBN 978-0-470-14831-0.

[11] GONÇALVES, Flávio E. Configuration guide for Asterisk PBX: how to build and configure a PBX with open source software featuring release 1.4. 2nd ed. s.l.: V.Office Networks, 2007. ISBN 978-85-906904-2-9.

[12] DUFFETT, David. Getting Started with Elastix: A Beginner´s Guide, 2013

[13] Home - Asterisk Project - Asterisk Project Wiki. 302 Found [online]. Dostupné z: https://wiki.asterisk.org/wiki/display/AST/Home

[14] Install:4.4.x:git [Kamailio SIP Server Wiki]. 302 Found [online]. Dostupné z: https://www.kamailio.org/wiki/install/4.4.x/git

[15] Elastix - Your Linux PBX Unified Communications Solution. Elastix - Your Linux PBX Unified Communications Solution [online]. Copyright © 2006 [cit. 09.04.2017]. Dostupné z: https://www.elastix.org/

[16] Cisco IOS Technologies - Cisco. Cisco - Global Home Page [online].

Dostupné z: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-technologies/index.html

[17] List of most popular softphones : Sippy Software, Inc. . [online]. Dostupné z: http://support.sippysoft.com/support/solutions/articles/127865-list-of-most-popular-softphones

Seznam příloh

Příloha na CD disku.

Adresářová struktura přiloženého CD disku:

Data: Pdf obsahující odkazy ke stažení vytvořených modelů, Pdf dokumentace k jednotlivým modelům.